生物特征加密基础

庞辽军　赵伟强　李岩
黄树杰　付青柳　靖毅　陈炯　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书以生物特征加密技术为背景，以生物特征中使用最为成熟和广泛的指纹特征为例，详细介绍了生物特征加密技术的相关概念和整体流程，并针对该技术中的每一个功能模块介绍了对应的经典算法。

内容包括：生物特征加密技术的基本概念以及指纹识别技术的发展历程；生物特征识别技术相关的图像处理基础知识；以指纹特征为例介绍了构成自动指纹识别系统的各个模块的实现方法和指纹识别算法的性能评价；生物特征识别技术与加密技术的结合方法；生物特征加密技术在当下的应用以及未来发展的展望。

本书可以作为高等院校相关专业的本科生及研究生教材，同时也可作为从事生物特征加密工作的科研人员的参考书目。

图书在版编目(CIP)数据

生物特征加密基础 / 庞辽军等编著. —北京：电子工业出版社，2016.2
ISBN 978-7-121-28071-9

Ⅰ. ①生… Ⅱ. ①庞… Ⅲ. ①个人鉴定(法医)－特征识别－加密技术 Ⅳ. ①D919.4②TN918.2

中国版本图书馆 CIP 数据核字(2016)第 011940 号

策划编辑：陈晓莉
责任编辑：陈晓莉
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1 092　1/16　印张：8.75　字数：224 千字
版　　次：2016 年 2 月第 1 版
印　　次：2016 年 2 月第 1 次印刷
定　　价：58.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：(010)88258888。

前　言

生物特征加密技术是当前信息安全领域的一个热点课题，它是基于生物特征识别技术和加密技术的相结合而发展的，其特点是兼顾了生物特征识别的唯一性和密码学的严谨性。生物特征加密技术将成为未来电子商务、电子政务及众多领域的重点发展技术。

生物特征识别技术由于其唯一性及稳定性等特点，已经成为世界各国科研人员的研究焦点。随着计算机技术与互联网的高速发展，生物特征识别技术已经成为当前信息技术领域炙手可热的研究方向之一。如今，生物特征识别技术已经成熟且广泛应用在社会活动的各个领域，如电子政务、电子商务、考勤管理以及移动终端应用等。成型的生物特征设备如考勤机、门禁等已经应用在许多办公场所中，许多国际知名手机厂商生产的智能手机中也使用了生物特征识别技术作为解锁和支付的新方法。

随着生物特征识别技术应用的愈加深入，其本身固有的一些缺陷和不足也逐渐暴露出来，最主要的就是生物特征所涉及的个人隐私以及由此而带来的安全性问题。生物特征是人所固有的，一旦丢失则存在非常大的风险。随着生物特征识别技术的普遍应用，它本身的安全问题也受到了重视，对生物特征本身的保护引发了许多研究课题。生物特征加密技术就是解决这类问题的新兴方法，它结合了生物特征识别技术和密码学技术的特点，保证了生物特征识别技术和加密技术在应用过程中的安全。

本书的特点是理论与应用并重。在介绍生物特征加密技术理论知识和基本概念的同时，结合实际应用，详细地介绍了最为常用的经典算法，并尽可能地辅以实例，能够让读者快速入门。

本书的编写结合了作者多年的科研经验，融入了作者在培养生物特征加密相关专业的研究生及本科生过程中总结的教学思路和教学方法，是一本反映生物特征加密技术教材。全书共分为 11 章，详细地介绍了生物特征加密技术框架中各个模块的概念和实现方法，并加入了大量的实例。

第 1 章为绪论，包括生物特征识别与加密技术简介、中国古代指纹的应用记载、西方指纹学的形成、指纹识别系统发展史和我国指纹识别技术发展史等内容。

第 2 章为基础知识与基本方法，包括图像和图像处理、图像中的变换、图像中的滤波、图像中的形态学处理、边缘检测等内容。

第 3 章为认识指纹图像，包括指纹图像概述、指纹图像描述、指纹的脊线特征等内容。

第 4 章为自动指纹识别系统及加密系统，包括自动指纹识别系统与加密系统框架、指纹图像的采集、指纹图像的预处理、指纹特征提取、指纹匹配和生物特征加密系统等内容。

第 5 章为指纹识别算法性能评价，包括指纹识别数据库、常规指纹识别算法性能评价，以及应用级指纹识别算法性能评价等内容。

第 6 章为指纹图像的采集，包括指纹采集的发展、指纹传感器的分类以及不同指纹传

感器的性能比较。

第 7 章为指纹图像分割，包括指纹分割概述、指纹分割指标计算、最小均方算法用于指纹分割和用于指纹分割的聚类方法等内容。

第 8 章为指纹图像增强与二值化，包括增强、基于 Gabor 滤波的增强算法、基于方向各向异性滤波的增强算法和二值化等内容。

第 9 章为指纹图像特征提取与匹配，包括传统的指纹特征提取与匹配算法、应用链码进行特征提取和方向场描述子(Tico)特征匹配等内容。

第 10 章为生物特征加密技术，包括生物特征加密技术发展概述、生物特征与密钥结合的常用方法、模糊保险箱算法介绍和指纹模糊保险箱算法实现等内容。

第 11 章为生物特征识别与加密技术的典型应用，包括电子政务领域的应用、移动终端的应用、电子商务的应用和应用展望等内容。

参加本书编写工作的有西安电子科技大学生命科学技术学院庞辽军、赵伟强、李岩、黄树杰、付青柳、靖毅和陈炯等人，其中庞辽军、赵伟强、李岩做出了主要的贡献，在此感谢参与编写本书的所有老师和研究生。

此外，本书的编写还要感谢西安电子科技大学教材建设重点项目(No. A1008)的资助。

由于编者水平所限，书中难免存在不足之处，敬请广大读者批评指正。

作者

2015 年于西安

目　录

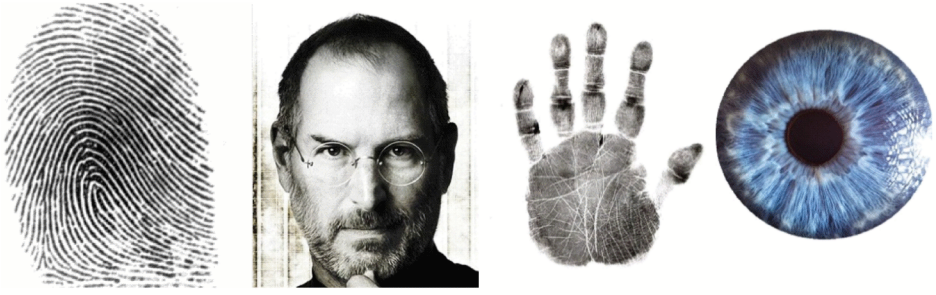
第1章　绪　　论

生物特征加密技术是生物特征识别技术和密码学技术相辅相成的新兴技术，其目的是将生物特征信息和密钥信息安全地结合在一起，该技术兼顾了生物特征识别的唯一性和密码学的严谨性，是信息安全领域的一个重要的发展趋势。本章对生物特征识别和加密技术进行简要介绍，并对使用最为广泛的指纹识别技术的发展进行详细的介绍。

本章的内容安排：1.1 节介绍生物特征识别与加密技术的概念；1.2 节介绍中国古代指纹应用记载；1.3 节介绍西方指纹学的发展史；1.4 节介绍指纹识别系统的发展史；1.5 节介绍我国指纹技术发展史；1.6 节总结本章的内容。

1.1　生物特征识别与加密技术简介

生物特征识别技术是基于人类生物特征来进行身份识别的技术。生物特征可以被分为生理特征和行为特征，生理特征包括指纹、人脸、掌纹以及虹膜等特征，如图 1-1 所示；行为特征包括步态、笔迹以及声音等特征如图 1-2 所示。



(a) 指纹特征　(b) 人脸特征　(c) 掌纹特征　(d) 虹膜特征

图 1-1　人类的生理特征

(a) 步态　(b) 笔迹　(c) 声音

图 1-2　人类的行为特征

生物特征是每个人自身所拥有的特征，因此相对于传统的个人身份识别方式，如携带身份证或记忆密码，生物特征识别更为安全和可靠，因为它不会丢失和遗忘。能够用于进行身份识别的生物特征一般拥有以下特点。

（1）普遍性：该特征是每个人都拥有的。

（2）唯一性：该特征因人而异，人与人之间不同。

（3）不变性：该特征稳定，不随时间而改变。

（4）易采集：该特征易于采集并能够数字化。

由于生物特征自身的特点，科研人员对生物特征识别技术进行了深入的研究。如今，生物特征识别技术已经发展成熟，并广泛地应用在刑侦鉴定、企业管理、出入境管理、金融服务、电子商务、信息安全、个人隐私保护等各个方面，生物特征识别技术拥有的市场规模也越来越大，图 1-3 显示了 2007—2020 年全球生物特征识别技术市场规模与预测（单位：亿美元）。在整个生物特征识别市场中，指纹识别技术的占有率超过了 50%，位居所有生物特征之首，图 1-4 显示了 2015—2020 年全球生物特征识别技术行业分类市场预测（单位：亿美元）。

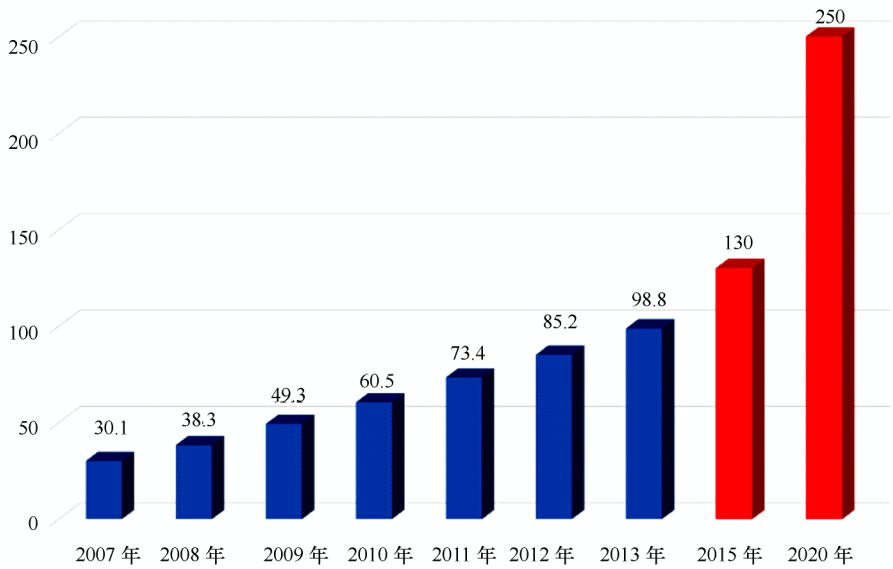


图 1-3　2007—2020 年全球生物识别技术行业市场规模与预测 单位：亿美元

随着生物特征识别技术应用的需求日益增加，其本身的安全性也引起了人们的重视，生物特征是人所固有的，它所涉及的个人隐私以及由此而带来的安全性问题不容忽视。因此，如何在方便地应用生物特征识别技术的同时保证生物特征的安全尤为重要。

密码学是研究信息系统安全保密的科学，是对信息进行编码以实现隐蔽信息的一门学问，被认为是解决信息安全问题的首要技术手段。一个密码算法通常包括加密和解密两个部分，加密和解密操作通常都是在一组密钥的控制下进行的，典型的密钥都是足够长且随机的，比如 AES 加密算法（Advanced Encryption Standard，高级加密标准）的密钥是 128 位的随机比特流，用户通常无法记忆如此长的密钥，所以密钥就会被保存在某种介质

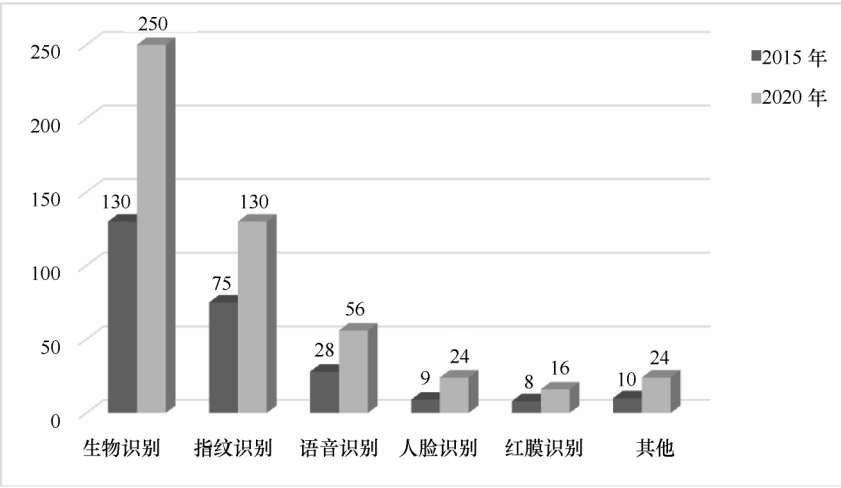


图 1-4　2015—2020 年全球生物特征识别技术行业分类市场预测 单位:亿美元

上,比如 U 盘或硬盘,然后再由一个相对容易记忆的口令来保护密钥,而口令由于其本身的非随机性和较小的长度,往往容易被攻击者破解,从而危及密码系统的安全。

生物特征加密技术结合了生物特征识别技术和密码学技术,将生物特征和密钥以某种方式结合起来,实现了基于密钥和生物特征的双重保护,使得攻击者既无法获取密钥也无法获取生物特征信息。

每一种生物特征都有其独有的特点,表 1-1 给出了不同生物特征之间的在不同性能指标上的简单比较。

表 1-1　不同生物特征的比较

生物特征	普遍性	独特性	永久性	可采集性	性能要求	可接受性	安全性
DNA	高	高	高	低	高	低	低
指纹	中	高	高	中	高	中	高
人脸	高	低	中	高	低	高	高
耳郭	中	中	高	中	中	高	中
虹膜	高	高	高	中	高	低	低
掌纹	中	高	高	中	高	中	中
声波	中	低	低	中	低	高	高
签名	低	低	低	高	低	高	低
步态	中	低	低	高	低	高	中

可以看出,没有一种生物特征是完全优于其它特征的。但综合来看,指纹技术更容易应用在各个领域,这也是指纹在生物特征识别市场中占最大份额的原因。由于生物特征加密的原理在应用不同生物特征时基本相似,而指纹技术的应用最为成熟,因此,本书将以指纹作为生物特征的实例,对生物特征加密进行详细介绍。如果不特别指出,本书后文中的生物特征指的就是指纹特征。

1.2 中国古代指纹应用记载

指纹技术起源于中国，据考古实物和史料记载已有数千年的历史。1927 年，德国指纹学家 Robert Heindl 就在其《指纹鉴定》一书中指出，中国唐代的贾公彦是世界上第一个提出用指纹识别人身份的学者。

在古代，指纹最早是作为陶器的一种装饰纹，在我国的西安半坡遗址、大汶口文化遗址、马家窑遗址等先后出土了带有指纹图案的陶器，如图 1-5(a)所示。随后，人们发现指纹各不相同，于是将其引入契约的签订当中，《周礼》中就有“以质剂而止讼”一语，图 1-5(b)显示了一份古代按有指纹的契约书。我国古代军队也有《箕斗册》，即登记士兵指纹以便检查，表明当时已能对指纹按形态、结构进行正确分类，并将这种分类特征和知识应用于社会实践。

我国将指纹用于刑侦的记录可追溯到两千多年前的秦代。1975 年出土的云梦秦竹简《封诊式・穴盗》记载“内中及穴中外壤有膝、手迹、膝，手各处”，即对现场勘查中的手印的描述。到了宋代，手印已正式成为刑事诉讼的物证了，《宋史・元绛传》中记载了一起欺诈案件，就是以指纹为依据来断案的。明代冯梦龙的《警世通言》第 33 卷《乔彦杰一妾破家》中也有类似记载：“安抚见洪三招状明白，点指画字”。

(a)指纹作为图案刻在陶器上　　(b)契约书上的指纹

图 1-5　中国古代指纹的使用

随着汉朝“丝绸之路”的开通，我国古代各朝与世界各国的交往也逐渐扩大，伴随着商业和法律制度的交流，指纹术相继传入到日本、印度以及阿拉伯地区和国家，并被多个国家在商业契约中广泛应用，为后来西方国家的指纹学奠定了重要基础。

1.3 西方指纹学的形成

指纹学是研究指纹表面生理特征、纹理结构及指纹收集、显现、储存、分类与识别的原理和方法的科学，指纹学作为一门学科被研究始于欧洲，是物证技术的一个重要组成部分。

自 17 世纪开始，西方一些医生和人类学者就对指纹进行了长期的潜心探索。1684 年，英国生理学家 Nehemiah Glue 在《哲学公报》上精确地描述了指纹的汗孔、皮肤脊线及排列方式，成为世界上第一个描写了微观指纹的人。

1858 年，英国人 William James Herschell 在印度、孟加拉采用中国商人在契约上按大拇指印的方法与土著人签订协议。在此之后，Herschell 又要求犯人们在入狱之前留下手印作为印记进行身份存档。1877 年，Herschell 写出了《手之纹线》，详细记述了他确认指纹是不会重复的实验结果。

1880 年，英国的 Henry Fauld 医生在《自然》杂志上发表第一篇有关指纹的研究，把指纹学从经验转移到以实验技术解剖学、胚胎学等为基础的科学轨道上。但在当时，Alphonse Bertillion 提出的人体测量法较为盛行，因此 Fauld 的指纹识别技术未能得到推广。但即便如此，西方学者普遍认为 Fauld 是西方近代指纹学的倡导者之一。

指纹学形成后，世界各地警方逐渐开始将指纹技术应用到案件侦破工作。1891 年，Francis Galton 提出了著名的高尔顿分类系统。随后，英国、美国、德国等国家的警察部门先后采用指纹鉴别法作为身份鉴定的主要方法。到了 20 世纪 60 年代，由于计算机可以有效地处理图形，人们开始着手研究利用计算机来处理指纹，美国联邦调查局(Federal Bureau of Investigation，FBI)和法国巴黎警察局开始研究开发自动指纹识别系统(Automated Fingerprint Identification System，AFIS)用于刑事案件侦破。此后，自动指纹识别系统在法律实施方面的研究和应用在世界许多国家展开。

到了 20 世纪 80 年代，随着个人计算机、光学扫描这两项技术的发展，指纹的获取变得更为便捷、高效，指纹识别系统得到了快速的发展，下一节我们将详细介绍指纹识别系统的发展史。

1.4　指纹识别系统发展史

指纹识别系统是一个从输入指纹图像到获取识别结果的完整系统，它的发展经历了手动指纹识别系统、半自动指纹识别系统和自动指纹识别系统三个阶段。

1.4.1　手动指纹识别系统的发展

手动指纹识别系统是利用统一的标准，人工对指纹形态进行分类标示，并描述出细节点等重要特征，将事先存储的指纹与实时采集的指纹进行比较，进而实现证实是否为同一指纹的目的。手工管理系统是指纹技术发展史上的关键环节，意味着指纹识别技术正式成为支撑刑侦破案的技术之一，广泛应用于 20 世纪初期至 70 年代，为以后的半自动管理系统和自动识别系统发展打下了坚实基础。

1888 年，阿根廷警官 Juan Vucetich 发表了《比较指纹学》一文，论述了指纹鉴定法的实用价值，并在 1892 年利用指纹比对成功地破获了一起案件：一个名为 Francisca Rojas 的女人残忍地将两个儿子割喉杀害，同时造成自己受伤的假象，并诬陷给自己的邻居，最终通过现场找到的她的指纹，揭示了真相。

1892 年,英国学者 Francis Galton 在《指纹学》一书中提出了“指纹稳定性和特定性、纹理分类和记录方法以及指纹鉴定技术”这三个影响重大的科学论点,即指纹终生不变、指纹可分类和指纹可识别。英国警官 Edward Richard Henry 在深入学习高尔顿的指纹学成果后,历经 7 年的试验,于 1900 年发表了《指纹的分类与功用》一文,使得指纹分类存储方法得到圆满解决,因其在高尔顿分类基础上制定,因此世人称为“高尔顿—亨利指纹鉴定系统”,该系统将指纹分为乎拱型、凸拱型、挠骨环状型、尸骨环状型、螺纹型 5 种类型。

1901 年,英国正式废除人体测量法,全面采用指纹鉴定法,并在警察机构成立专门的指纹部门,在指纹识别应用的一年时间内就查处前科罪犯 1772 人。从此以后,手动指纹识别系统在世界各国广泛应用。1939 年开始,美国联邦调查局改制之后的第一任局长 Edgar Hoover 对鉴识部的指纹档案进行了扩充及合并,建成了当时世界上最大手动指纹识别数据库。

随着计算机技术的发展和指纹数据库的增大,手动指纹识别系统已经不能满足需求,人们的目光转向了利用计算机的半自动指纹系统,下一节我们将介绍半自动指纹系统。

1.4.2 半自动指纹识别系统

半自动指纹识别系统是借鉴先进的计算机技术,将指纹输入到计算机中,人工使用分析仪对指纹进行分类编码后存储,利用计算机的存储和快速计算的优势,实现高效的指纹比对和鉴定。较手动识别相比,半自动指纹识别具有效率高、存储量大的特点,并广泛应用于 20 世纪 70 年代至 80 年代末期。

20 世纪 70 年代,随着计算机技术在各科学领域中的逐渐应用,德国、日本、南斯拉夫等国家开始将计算机应用到指纹管理和比对,利用摄像机将指纹图像输入到计算机系统,采用人工编码方式进行分类,人工确定指纹中心、细节点的位置和方向,实现了半自动指纹识别模式。

半自动指纹识别系统充分发挥了计算机运算速度快而稳定的优势,有效地提高了指纹查档速度和精度,使指纹档案管理更加科学、实用。但随着指纹数据库中指纹数量的日趋增多,半自动指纹识别系统的工作效率降低,并且出现管理成本和人工成本大幅增加的瓶颈,为自动指纹识别系统的发展埋下了伏笔。

1.4.3 自动指纹识别系统的发展

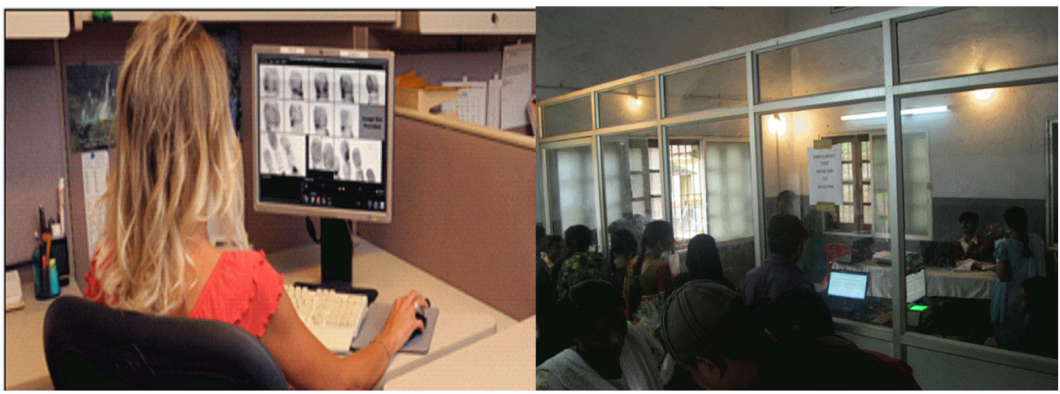
自动指纹识别系统是以指纹自动处理为核心的指纹处理、管理、识别的计算机系统,依托先进的计算机和软件技术,实现指纹的自动分类、定位、特征提取和比对等,以其存储量大、比对速度快、效率高等优越性,促进现代指纹技术产生质的飞跃。自动指纹识别系统从 20 世纪 70 年代开始使用并广泛应用至今。

1963 年,美国联邦调查局提出了自动指纹识别系统的设想,在参考手动指纹识别系统的基础上,综合计算机和模式识别技术,设计了能够对指纹进行图像采集、特征匹配和

自动筛选的计算机管理系统，并于 20 世纪 70 年代率先研制成功。80 年代，德、日等国家认识到半自动指纹管理系统的人工编码存在效率低的问题，无法应付日趋庞大的指纹数据，因此也开始发展指纹自动识别系统。自 80 年代末期，西方各国逐渐淘汰了自动化水平较低的半自动管理系统，开始使用自动指纹识别系统，从此自动指纹识别系统开始蓬勃地发展起来。

到目前为止，作为指纹识别应用最成功的例子，美国联邦调查局建立了一个国家级指纹和犯罪记录查找系统——IAFIS(The Integrated Automated Fingerprint Identification System)，该数据库在 2009 年已拥有超过 7 亿的罪犯指纹和 3.4 亿公民指纹，是当时世界上最大的生物特征数据库，图 1-6(a)是一名正在进行指纹数据分析的 FBI 雇员。

印度的身份识别项目(Unique Identification project，也称“Aadhar”计划)已完成了对逾 5 亿人的人口统计与生物识别数据采集工作，图 1-6(b)显示了印度居民录入指纹的场景。预计将剩下的 7 亿人纳入此数据库系统后，该数据库总量将达到皮比特(petabytes)级别。



(a) FBI 雇员正在进行 IAFIS 系统的指纹分析工作　　(b) 印度居民正在采集指纹

图 1-6　各国自动指纹系统的研究

我国也在积极建设公民生物特征数据库，截至 2014 年 8 月份，全国已有超过 16000 个派出所启动了居民二代身份证指纹信息录入工作。

1.5　我国指纹技术发展史

在我国，由于封建社会的体制等原因，科学技术未能取得应有的社会地位，发源于我国的指纹术也未得到科学性的发展。清朝末年，随着封建社会的衰落，西方各国纷纷到中国强占租界，并在租界内推行各自的指纹管理方法，如英国在香港和上海租界推行亨利式指纹管理制度、德国在青岛推行汉堡式指纹管理制度、法国在上海租界推行爱蒙培尔指纹制度等。虽然西方列强的行为对我国人民造成了伤害，但从指纹识别技术的发展角度讲，这种指纹管理制度的推行，或多或少推动了指纹技术在我国的发展。

国民党统治初期，各地警察局纷纷采用国外的指纹管理制度，在应用中遇到许多障碍。1930 年，刘紫菟设计出中华式指纹分类法，但因无法摆脱列强控制，终归无法付诸实

施。1942 年,国民党警察总署做出了统一全国指纹制度的决议,1948 年决定十指指纹分析法采用亨利制度,单指纹采用伯特利制度,但因人民解放战争的胜利,此决议未能实行。同年,我党在东北解放区接收日本人建立的指纹档案后,在哈尔滨成立了我国第一个完整规范的指纹室。

新中国成立后,我国花费数年时间不断摸索完善了指纹管理及其相关专业人才培养的制度,最终于 1956 年确定我国建立统一的十指指纹分析和管理方法,从而实现了规范的、统一的、科学的中华民族的十指指纹分析法和系统管理机构,单指纹管理方法也在各地市纷纷应用。

20 世纪 80 年代初期,我国受资金、技术等因素所限,未能直接购买西方国家先进的自动指纹识别系统,开始了半自动指纹识别系统的研发与应用,全国先后推出 10 余种半自动指纹管理系统,覆盖了全国近半数地市,取得了良好的应用效果,同时积累了许多指纹管理经验和指纹搜集、管理机制。一些高校以及公安科研部门也对自动识别系统进行了研究和探索。随着指纹数据库的日益庞大,半自动指纹识别系统的局限性也逐渐暴露,指纹编码速度、比对的准确性和效率远不能满足工作之需。90 年代初期,各地市纷纷停止了半自动指纹系统的应用。90 年代中期,随着计算机技术、模式识别理论和刑事科学技术的进一步发展,我国成功研发了多套自动指纹识别系统,比较出名的有北京大学的 Delta-S 系统、清华大学的 CAF-Is 系统等,与此同时,国外的自动指纹识别系统价格也大幅下降,1997 年全国各地市开始大范围应用自动指纹识别系统,主要包括美国 COGENT、日本 NEC、法国 Morpho 等系统。

目前,全国各地市采集、存储十指指纹约近亿份(10 个指纹为 1 份),现场指纹近千万枚,年破案在 20 万起以上,效果显著。随着全民指纹捺印时代已经来临,必将给指纹管理和刑侦破案工作带来跨越式的发展。

1.6 本章小结

本章对生物特征识别与加密技术进行了介绍。作为生物特征识别技术中应用最成熟的技术,我们对指纹识别技术和指纹识别系统在国内外的发展进行了详细的介绍。本章让读者对生物特征加密技术和指纹识别技术有大概的了解,部分涉及历史的内容仅供参考,有出入的地方请读者不必深究,我们的重点将放在后边对生物特征识别技术方法的介绍上。

习题与思考题

1. 为什么起源于我国的指纹术却在欧洲得到了快速的发展?
2. 为什么亨利·富尔兹被认为是近代指纹学的倡导者之一?
3. 为什么指纹可以作为证物运用在古代破案中?
4. 你认为指纹特征在生物特征识别中会继续独占鳌头吗?为什么?
5. 你认为自动指纹识别系统会在司法程序中完全取代半自动或手动指纹识别系统吗?请说明原因。

第 2 章　基础知识与基本方法

本章针对自动指纹识别系统介绍数字图像处理的一些基础知识和基本方法。在生物特征识别算法中,生物特征信息一般通过图像来进行存储并与待识别的生物特征信息来进行比对。自动指纹识别技术的发展是随着数字图像处理和模式识别等学科的发展而兴起的,自动指纹识别系统首先通过采集仪获得指纹图像,一般为灰度图像,然后对灰度指纹图像进行分割、增强、特征提取及匹配等处理,进而得到识别结果。在这一系列处理中,数字图像处理的基础知识和基本方法扮演了重要角色,这些基础知识和基本方法是指纹识别的技术基础。

本章的内容安排:2.1 节主要讲数字图像、图像评估以及数字图像处理的概念及应用;2.2 节详细介绍了数字图像处理中常用的傅里叶变换和霍夫变换;2.3 节重点介绍了数字图像处理中常用的高斯滤波器和中值滤波器;2.4 节围绕腐蚀、膨胀、开闭运算等形态学操作展开介绍;2.5 节主要讲了边缘检测的几种常用方法;2.6 节对本章进行总结。

2.1　图像和图像处理

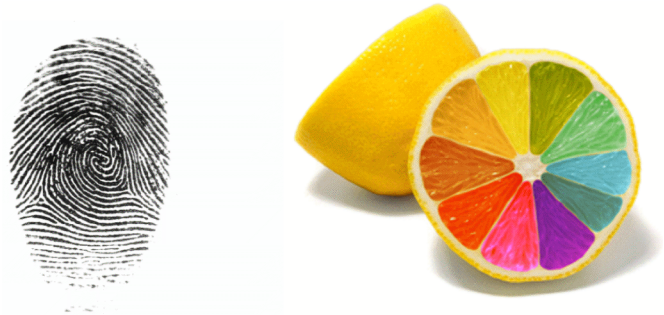
图像是指利用采集设备对客观的三维世界的实体以及环境进行数据采集所得到的结果。图像与人类活动关系非常密切,已经获得广泛应用的自动指纹识别系统也是以指纹图像为载体进行构建的。除了指纹识别的应用,从日常家庭生活到生产、医疗、艺术、文教、军事和航天等都离不开图像。这种迫切的实际需求给图像处理技术的发展提供了巨大的动力,促进了图像处理技术的发展。

2.1.1　数字图像

数字图像由二维的元素组成,每一个元素具有一个特定的位置和灰度值,这些元素称为像素。因为模拟图像的点都是连续的,所以计算机无法接受模拟形式的图像。为了便于计算机处理和表达,我们将模拟图像转化为可以用计算机进行处理的数字图像,这种转化就是图像的数字化。一幅模拟图像经过采样和量化使其在空间上和数值上都离散化,形成一个数字点阵,通常采用等间隔采样和均匀量化的方法。

图像可以分为多种类型。当图像内容随时间变化时,称之为时变图像或运动图像。当图像内容不随时间变化时,称之为静止图像。由于在指纹图像处理过程中涉及的都是静止图像,因此我们将会重点介绍静止图像。对于静止图像,若不考虑光的波长只考虑光的能量,在视觉上只有黑白深浅之分,没有彩色变化,这时称为灰度图像。当考虑不同波长的光时,则为彩色图像。如图 2-1 展示了灰度图像与彩色图像,其中图(a)为灰度图像,图(b)为彩色图像。

对于灰度图像而言,可以采用二元组公式(2-1)来表示。



(a) (b)

图 2-1 灰度图像与彩色图像

$$I=f(x,y) \tag{2-1}$$

式(2-1)中(x,y)表示二维平面上的点,$1\leqslant x\leqslant M-1$,$1\leqslant y\leqslant N-1$。$M$ 和 N 分别表示图像在水平及垂直方向的最大尺度。函数值 $f(x,y)$ 表示(x,y)位置处像素的灰度值,其范围通常在 0～255 之间,0 代表黑色,255 代表白色。灰度值可以认为是亮度,其数值表示像素的灰度信息,即图像像素的深浅程度。图像的灰度等级是灰度图像具有的灰度种类的数目,通常使用的灰度等级有三种:256,16 和 2。

灰度等级也可以用位深来表示。位深,也称作位分辨率,代表图像中一个像素占有的二进制位数。例如,对于具有 256 个强度等级的图像来说,其位深为 8,也称为 8 比特图像。图像的位深越大,图像的灰度范围就越广,所描述的内容就越精细。

图 2-2 为两个具有 256 个强度等级的指纹灰度图像实例,其中,图(a)为 FVC(Fingerprint Verification Competition)2004 数据库中的指纹图像,大小为 640×480,位深为 8;图(b)为 FVC 2006 数据库中的指纹图像,大小为 96×96,位深为 8。两幅图像中每一个像素点都对应一个 0～255 之间的灰度值。

(a) (b)

图 2-2 指纹图像

2.1.2 图像质量评估

自动指纹识别系统对指纹的质量有一定的要求,而指纹采集过程中采集到的指纹质

量可能不同，这就要求我们需要对指纹质量进行评估。一方面，如果指纹质量过差，我们可以选择重新采集指纹；另一方面，我们可以找到指纹中质量较好的区域并重点利用这些区域的特征信息来进行识别处理。

在数字图像处理过程中，所有技术的优劣都会影响到图像的质量。图像质量的含义主要包括图像的逼真度和可懂度两个方面的内容。为了对图像处理的各个环节进行合理的评估，图像质量评价的研究已经成为图像信息工程的基础之一。

在传统的图像质量评价方法中，有代表性的方法主要有两种：客观评价和主观评价。对图像质量进行客观评价，实际上是通过与该图像有关的客观参数的大小来反映出图像的好坏。由于在很多应用中，图像最终是给人看的，所以需要以人的主观评价来对图像质量进行判断。

国际上已有成熟的主观评价技术和国际标准，例如，ITU-T Rec. P. 910 规定了多媒体应用的主观评价方法；ITU-R BT. 500—11 规定了电视图像的主观评价方法，其就视频质量主观评价过程中的测试序列、人员、距离以及环境做了详细规定。主观质量评分法(Mean Opinion Score，MOS)是图像质量最具代表性的主观评价方法。而主观质量评分法又可以分为绝对评价和相对评价两种类型。

绝对评价是将图像直接按照视觉感受分级评分，表 2-1 列出了国际上规定的 5 级绝对尺度，包括质量尺度和妨碍尺度。对一般人来讲，多采用质量尺度；对专业人员来讲，则多采用妨碍尺度。

表 2-1　绝对评价表

分数	质量尺度	妨碍尺度
5 分	丝毫看不出图像质量好坏	非常好
4 分	能看出图像质量好坏但不妨碍观看	好
3 分	清楚看出图像质量好坏，对观看稍有妨碍	一半
2 分	对观看有妨碍	差
1 分	非常严重的观看妨碍	非常差

相对评价是由观察者将一批图像从好到坏进行分类，将它们相互比较得出好坏，并给出相应的评分。相对尺度如表 2-2 所示。

表 2-2　相对尺度表

分数	相对测量尺度	绝对测量尺度
5 分	一群中最好的	非常好
4 分	好于该群中平均水平的	好
3 分	该群中的中间水平	一般
2 分	差于该群中最差水平的	差
1 分	该群中最差的	非常差

对图像的质量评价方法和评价策略也可以应用在指纹图像中。在质量较好的滚动指纹中，大约有 70～80 个细节点，在局部指纹或者现场指纹中，细节点就少了很多，大约有 20～30 个。

图 2-3 展示了不同质量的指纹图像，其中，图(a)为清晰的滚动指纹图像，图(b)为较清晰的全指纹图像，图(c)为质量差的现场指纹图像。

(a)　　(b)　　(c)

图 2-3　不同质量的指纹图像

2.1.3　图像处理及应用

数字图像处理最早出现于 20 世纪 50 年代，当时的电子计算机已经发展到一定水平，人们开始利用计算机来处理图形和图像信息。数字图像处理作为一门学科大约形成于 20 世纪 60 年代初期。早期的图像处理的目的是改善图像的质量，它以人为对象，以改善人的视觉效果为目的。

数字图像处理系统由三部分组成，即图像采集及数字化设备，图像信息处理设备，图像显示及记录设备。图像的采集工具包括照相机、扫描仪等；图像信息的处理工作一般由计算机来完成；图像的显示设备包括永久显示设备，如打印机、照片等，以及暂时显示设备，如 CRT(Cathode Ray Tube)、LED (Light Emitting Diode)等。数字图像处理系统的构成如图 2-4 所示。

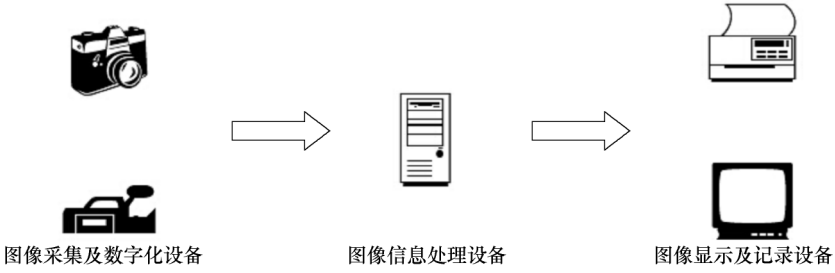


图 2-4　数字图像处理系统

图像以数字形式进入计算机，是进行数字图像处理的第一步。一幅灰度图像可以看成一个二维离散函数 $f(x,y)$，其灰度值表现为位置(x,y)处的函数值。计算机中的数字图像就是以矩阵形式表示的。不同的处理就是用不同的算法对这一图像矩阵进行运算。

数字图像处理系统中最核心的步骤是利用计算机对各种图像进行的相关处理。它涉及图像处理、模式识别和计算机视觉中的许多概念和方法。根据抽象程度的不同可把这些处理分为低、中、高三个层次。

低层处理涉及对图像进行加工以改善图像的视觉效果，或对图像数据进行压缩以利于图像的存储和传输。典型的处理方法有：图像对比度增强、边缘锐化、去噪声等。这些都是典型的图像增强处理，处理后的图像看起来更清楚。

中层处理主要是指用某种特殊的手段提取、描述和分析图像中所包含的某些特征或特殊的信息。这些特征包括很多方面，如图像的频域特征、灰度特征、边界特征、颜色特征、纹理特征、形状特征、拓扑特征以及关系结构等。这种处理往往要先进行图像分割，把感兴趣的对象从图像中分割出来，然后对它的特征进行测量，用特征数据来表示它，或用一些符号来表示对象或多个对象间的关系。中层处理的主要目的是便于计算机对图像做进一步的分析和理解，经常作为模式识别，计算机视觉等的预处理，指纹图像的分割增强等步骤就是属于中层处理的范畴。

高层处理涉及在图像分析中对被识别物体的总体理解。通过对图像内容的理解及对场景的解释，进而指导和规划行动。

除了按抽象程度对数字图像处理分为不同的层次，我们还可以从研究内容出发将数字图像分为以下几个方面。

1. 图像变换

由于图像阵列很大，直接在空间域中进行处理，涉及的计算量很大。因此，往往采用各种图像变换的方法，如傅里叶变换、沃尔什变换、离散余弦变换等间接处理技术，将空间域的处理转换为变换域处理，不仅可减少计算量，而且可获得更有效的处理结果（如傅里叶变换可在频域中进行数字滤波处理）。

2. 图像编码压缩

图像编码压缩技术可减少描述图像的数据量（即比特数），以便节省图像传输、处理时间和减少所占用的存储器容量。压缩可以在不失真的前提下获得，也可以在允许的失真条件下进行。编码是压缩技术中最重要的方法，它在图像处理技术中是发展最早且比较成熟的技术。

3. 图像增强和复原

图像增强和复原的目的是为了提高图像的质量，如去除噪声，提高图像的清晰度等。图像增强不考虑图像降质的原因，突出图像中所感兴趣的部分。例如，强化图像高频分量，可使图像中物体轮廓清晰，细节明显；又如强化低频分量可减少图像中噪声影响。图像复原要求对图像降质的原因有一定的了解，一般来讲应根据降质过程建立“降质模型”，再采用某种滤波方法，恢复或重建原来的图像。

4. 图像分割

图像分割是将图像中有意义的特征部分提取出来，其有意义的特征有图像中的边缘、区域等，这是进一步进行图像识别、分析和理解的基础。虽然目前已研究出不少边缘提取、区域分割的方法，但还没有一种普遍适用于各种图像的有效方法。因此，对图像分割的研究还在不断深入之中，是目前图像处理中研究的热点之一。

5. 图像描述

图像描述是图像识别和理解的必要前提。作为最简单的二值图像可采用其几何特性

描述物体的特性，一般图像的描述方法采用二维形状描述，它有边界描述和区域描述两类方法。对于特殊的纹理图像可采用二维纹理特征描述。随着图像处理研究的深入发展，已经开始进行三维物体描述的研究，提出了体积描述、表面描述、广义圆柱体描述等方法。

6. 图像分类(识别)

图像分类属于模式识别的范畴，其主要内容是图像经过某些预处理(增强、复原、压缩)后，进行图像分割和特征提取，从而进行判决分类。图像分类常采用经典的模式识别方法，有统计模式分类和句法(结构)模式分类，近年来新发展起来的模糊模式识别和人工神经网络模式分类在图像识别中也越来越受到重视。

从上文的介绍中我们可以看到，数字图像处理的研究涵盖了很多方面，也从侧面展示了数字图像处理广泛的应用前景。在工业自动控制中，可以利用数字图像处理系统进行纺织品的质量的检查、监视零部件的装配；在港口，可以利用数字图像处理系统检测调度，进行交通管理；在军事、公安等应用领域，数字图像处理系统可用于目标的侦探和目标识别跟踪制导，如基于图像匹配的巡航导弹等。下面我们将会从具体的基础方法出发，详细讲解与指纹识别处理相关的数字图像处理方法。

2.2 图像中的变换

对生物特征进行处理时，一般需要对模板图像进行一些变换，以方便后续识别工作，从而提高生物特征识别的速度与准确性。一般称原始图像为空间域图像，称变换后的图像为变换域图像，变换域图像可以反变换为空间域图像。例如，指纹识别过程中，经常需要对指纹图像做相关图像变换处理。本节中详细介绍两种在指纹识别处理中常用的两种变换：傅里叶变换(Fourier transform)和霍夫变换(Hough transform)。

2.2.1 傅里叶变换

傅里叶变换是数字图像处理变换中的重要部分，以指纹图像为例，通过傅里叶变换我们可以将空间域上的指纹图像信息转换为频率域上的指纹图像信息，在后续的滤波过程中避免了复杂的卷积运算，在指纹图像处理中有着重要的意义。

傅里叶变换将时域信号分解为不同频率的正弦信号或余弦信号叠加之和。法国数学家傅里叶指出：任何周期函数都可以表示为不同频率的正弦和或余弦和的形式。无论函数多么复杂，只要它是周期的，并且满足某些适度的数学条件，都可以用这样的和来表示。甚至非周期函数也可以用正弦或余弦乘以加权函数的积分来表示。这种情况下的公式就是傅里叶变换。用傅里叶级数或变换表示的函数特征完全可以通过傅里叶反变换来重建，而不会丢失任何信息。它可以使我们工作于“傅里叶域”，而且在返回到函数的原始域时不会丢失任何信息。总之，傅里叶变换是解决实际问题的有效工具，它作为基础工具被广泛的学习和使用。

连续情况下，要求原始信号在一个周期内满足绝对可积条件。非周期性连续时间信号 $x(t)$的傅里叶变换为公式(2-2)：

$$X(\omega)=\int_{-\infty}^{\infty}x(t)\mathrm{e}^{-\mathrm{j}\omega t}\,\mathrm{d}t \tag{2-2}$$

离散情况下,傅里叶变换一定存在。冈萨雷斯版《数字图像处理》里面的解释非常形象:一个恰当的比喻是将傅里叶变换比作一个玻璃棱镜。棱镜是可以将光分解为不同颜色的物理仪器,每个成分的颜色由波长(或频率)来决定。傅里叶变换可以看作是数学上的棱镜,将函数基于频率分解为不同的成分。当我们考虑光时,讨论它的光谱或频率谱。同样,傅里叶变换使我们能通过频率成分来分析一个函数。

由于数字图像是离散的,在实际应用中我们一般使用一维离散傅里叶变换和二维离散傅里叶变换。一维离散傅里叶变换的公式为

$$F(u)=\frac{1}{M}\sum_{X=0}^{M-1}f(x)\mathrm{e}^{-\mathrm{j}2\pi ux/M} \tag{2-3}$$

其中,$u=0,1,2,\cdots,M-1$。

二维离散傅里叶变换的为

$$F(u,v)=\frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\mathrm{e}^{-\mathrm{j}2\pi(ux/M+vy/N)} \tag{2-4}$$

其中,$u=0,1,2,\cdots,M-1$;$v=0,1,2,\cdots,N-1$;$f(x,y)$是大小为 $M\times N$ 的数字图像。

上边给出的离散傅里叶变换公式,理解起来较为抽象。要想更加透彻的掌握傅里叶变换,我们先要理解图像在频域中的意义。在频域中,频率越大说明原始信号变化速度越快;频率越小说明原始信号越平缓。当频率为 0 时,表示为直流信号,没有变化。因此,频率的大小反映了信号的变化快慢。高频分量解释信号的突变部分,而低频分量决定信号的整体形象。在图像处理中,频域反映了图像在空域灰度变化剧烈程度,也就是图像灰度的变化速度,也就是图像的梯度大小。对图像而言,图像的边缘部分是突变部分,变化较快,因此反映在频域上是高频分量,图像的噪声大部分情况下是高频部分,图像平缓变化部分则为低频分量。

理解了图像在频域中的意义,我们就能明白傅里叶变换其实是提供了另外一个角度来观察图像,将图像从灰度分布转化到频率分布上来观察图像的特征,傅里叶变换提供了一条从空域到频域自由转换的途径。通过傅里叶变换,既可以获得信号的频域特性,又可以将卷积运算转换为乘积运算。因此,傅里叶变换在图像处理的以下几个方面都有重要作用:

(1) 图像增强与图像去噪。绝大部分噪声都是图像的高频分量,通过低通滤波器来滤除高频噪声;边缘也是图像的高频分量,可以通过添加高频分量来增强原始图像的边缘。

(2) 图像分割与边缘检测,用于提取图像高频分量。

(3) 图像特征提取,如傅里叶描述与特征,它是一种形状特征,可以直接通过傅里叶系数计算得到。

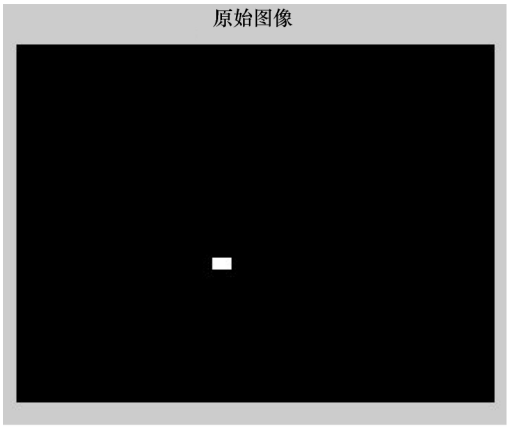
(4) 图像压缩。可以直接通过傅里叶系数来压缩数据,常用的离散余弦变换是傅里叶的实变换。

上边介绍了傅里叶变换的定义以及一些具体的应用,在图像处理的实际应用过程中,

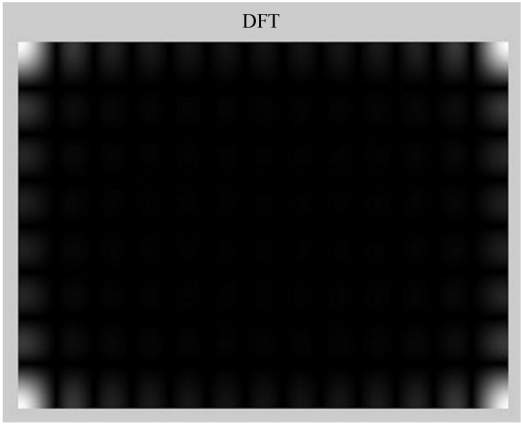
由于直接求取离散二维傅里叶变换计算量过大、复杂度过高，我们一般采用快速傅里叶变换方法来计算离散二维傅里叶变换。

快速傅里叶变换(FFT)是离散傅里叶变换的快速算法，它是根据离散傅里叶变换的奇、偶、虚、实等特性，对离散傅里叶变换的算法进行改进获得的。快速傅里叶变换 FFT 的基本思想是把原始的 N 点序列，依次分解成一系列的短序列，进而求出这些短序列相应的 DFT 并进行适当组合，达到删除重复计算，减少乘法运算和简化结构的目的。

下面是一个 DFT 变换实例，在图 2-5 中，图(a)为原图，图(b)为 DFT 变化后的图像。



(a)



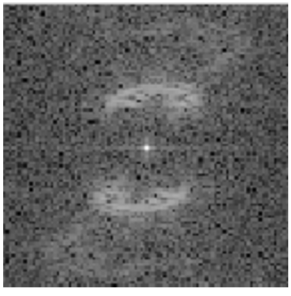
(b)

图 2-5　DFT 变换前后的图像

从图像中可以观察到，变换之后的图像在原点平移之前四角是低频，最亮。这可以通过对图像经过二维傅里叶变换后得到的变换系数矩阵分析后进行解释：若变换矩阵原点设在中心，其频谱能量集中分布在变换系数短阵的中心附近。若所用的二维傅里叶变换矩阵的原点设在左上角，那么图像信号能量将集中在系数矩阵的 4 个角上。这是由二维傅里叶变换本身性质决定的。

这里，我们还是通过一个指纹图像为实例来展示傅里叶变换的具体效果。在图 2-6 中，图(a)为原始指纹图像，图(b)为傅里叶变换以后的图像，通过傅里叶逆变换还可以得到原图(a)。

(a) 原指纹图像



(b) 傅里叶变换后的图像

图 2-6　傅里叶变换

2.2.2　霍夫变换

霍夫变换(Hough Transform)是图像处理中从图像中识别几何形状的基本方法之一,在自动指纹识别系统的匹配模块中有着重要的应用。霍夫变换的基本思想是在原始图像坐标系下的一个点对应了参数坐标系中的一条直线,同样参数坐标系的一条直线对应了原始坐标系下的一个点。原始坐标系下呈现直线的所有点,它们的斜率和截距是相同的,所以它们在参数坐标系下对应于同一个点。这样在将原始坐标系下的各个点投影到参数坐标系下之后,看参数坐标系下有没有聚集点,这样的聚集点就对应了原始坐标系下的直线。

霍夫变换的意义在于利用点与线的对偶性,将原始图像空间给定的曲线通过曲线表达形式变为参数空间的一个点。这样就把原始图像中给定曲线的检测问题转化为寻找参数空间中的峰值问题,亦即把检测整体特性转化为检测局部特性,比如可以将霍夫变换推广为检测直线、椭圆、圆、弧线等。

例如,在图像中检测直线的问题,其实质是找到构成直线的所有的像素点。那么问题就从找到直线,变成找到符合 $y=mx+C$ 的所有(x,y)的点。进行坐标系变化,将直线 $y=mx+C$[如图 2-7(a)所示]变成直线 $c=-xm+b$[如图 2-7(b)所示]。直线上的点(x_1,y_1),在转换坐标系后为一条直线。如图 2-7 所示,直线上每一个点在 mc 坐标系中都表现为直线,而且这些直线都相交于一个点,即(m,c)。找到所有点的问题,转变为寻找直线的问题。对于图像中的每一个点,在 mc 坐标系中对应着很多的直线。找到直线的交点,就对应着找到了图像中的直线。

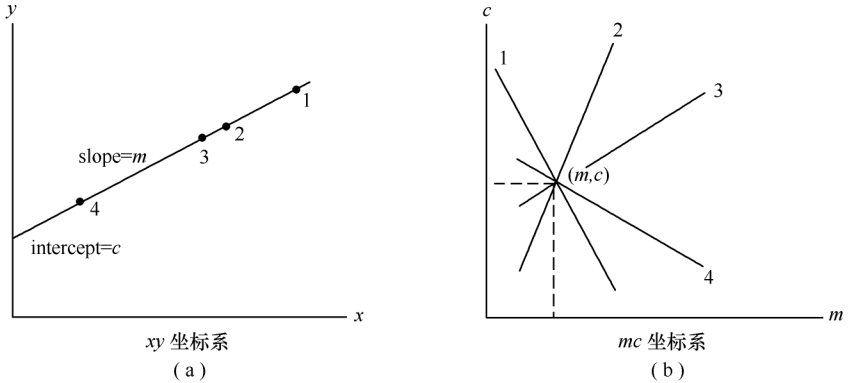


图 2-7　霍夫变换检测直线

通常的霍夫变换可以推广至点的匹配。我们将所有可能的转换集合离散化,对每一个可能的转换,计算其匹配分数,得分最高的转换被认为是正确的转换。这种方法可以应用到指纹图像的对准过程中,关于指纹方面的一些基础知识请参见第 3 章,霍夫变换在指纹图像对准中的具体策略如下:

我们认为转换 $F_{s,\theta,\Delta x,\Delta y}:R^2\rightarrow R^2$ 可以由式(2-5)得出

$$F_{s,\theta,\Delta x,\Delta y}\begin{pmatrix}x\\y\end{pmatrix}=s\begin{pmatrix}\cos\theta & \sin\theta\\-\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}\Delta x\\\Delta y\end{pmatrix} \tag{2-5}$$

其中，s、θ 和 Δx、Δy 分别表示尺度、旋转和平移参数，要对两幅指纹图像进行对准，这些参数都是需要计算出来的。

转换结果的匹配分数存储在数组 A 中，$A(k,l,m,m)$记录 $F_{s,\theta,\Delta x,\Delta y}$转换的可信度，$A$ 是由以下方法得到的。对每一对(p,q)，$p=(p_x^i,p_y^i)$是 P 集合中的一个点，而 $q=(q_x^i,q_y^i)$是集合 Q 中的一个点，用其来增加数组 A 中转换的可信度。对每一对(s_k,θ_l)值，都有一个准确的平移向量$(\Delta x,\Delta y)^t$以使得 $F_{s,\theta,\Delta x,\Delta y}(p)=q$，这个平移向量的计算方法如式(2-6)：

$$\begin{pmatrix}\Delta x\\\Delta y\end{pmatrix}=q-s_k\begin{pmatrix}\cos\theta_1 & \sin\theta_1\\-\sin\theta_1 & \cos\theta_1\end{pmatrix}p \tag{2-6}$$

这样我们就可以求出旋转平移等参数，进而可以进行指纹图像的对准操作。我们也可以用一段伪代码来简单表示这个过程：

```
Procedure Hough
A(k, 1, m, n) := 0,
k = 1, …, K;
1 = 1, …, L;
m = 1, …, M;
n = 1, …, N
For(p_x, p_y, α)∈p do
        For(q_x, q_y, β)∈Q do
            Forθ∈{θ_1, …, θ_L} do
                If α+θ=βthen
                    For s∈ { s_1, …, s_L } do

                        (Dx)   (cosq_1   sinq_1)
                        (Dy) = q − s_k (−sinq_1  cosq_1) p
                        Add evidence for F_{s_k, θ_1, Δx, Δy}
                End for
            End if
        End for
    End for
End for
Result:= arg max_{k,l,m,n} A(k, 1, m, n)
EndHough
```

2.3 图像中的滤波

在自动指纹识别系统中，滤波也是对指纹图像进行处理的一种重要手段，例如，可以通过高斯滤波平滑图像，利用中值滤波去掉图像中的椒盐噪声。滤波就是在时域内做模

板运算，对图像进行卷积。模板运算是图像处理中一个很重要的处理过程，很多图像处理过程中都要用到。根据卷积定理，时域卷积等价与频域乘积。因此，在时域内对图像做模板运算就等效于在频域内对图像做滤波处理。比如说一个均值模板，其频域响应为一个低通滤波器；在时域内对图作做均值滤波就等效于在频域内对图像用均值模板的频域响应对图像的频域响应做一个低通滤波。

在数字图像处理中，最典型的方法就是空间域卷积，或称“开窗”运算，也称“模板”运算。若已知数字图像 $\boldsymbol{f}(m,n)$和空间处理模板或掩模(Mask)为

$$\begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix}$$

则模板运算处理对应于式(2-7)：

$$\boldsymbol{g}(m,n)=\boldsymbol{f}(m-1,n-1)m_{11}+\boldsymbol{f}(m-1,n)m_{12}+\cdots+\boldsymbol{f}(m+1,n+1)m_{33} \tag{2-7}$$

即处理结果只与模板和 $f(m,n)$以及其 8 个空间邻域的值有关。

如果令

$$\boldsymbol{h}(m,n)=\begin{bmatrix} m_{33} & m_{32} & m_{31} \\ m_{23} & m_{22} & m_{21} \\ m_{13} & m_{12} & m_{11} \end{bmatrix}$$

则式(2-7)可以写成式(2-8)所示离散卷积的形式：

$$\boldsymbol{g}(m,n)=\boldsymbol{f}(m,n)*[\boldsymbol{h}(m,n)] \tag{2-8}$$

用不同的滤波器可以直接在空间域进行边缘增强、噪声平滑和边缘检测等处理，接下来我们会重点介绍在自动指纹识别系统中一些常用的滤波方法。

2.3.1　中值滤波器

中值滤波也称中值平滑，是一种空间域非线性滤波技术，属于统计排序滤波器。这种滤波器的响应以滤波器包围的图像区域中所包含的像素的排序为基础，然后使用统计排序结果决定的值代替中心像素值，中值滤波器则是将像素邻域内灰度的中值代替该像素的值。中值滤波器的使用非常普遍，因为对一定类型的随机噪声，它提供了一种优秀的去噪能力，而且比相同尺寸的线性平滑滤波器的模糊程度明显要低。对于椒盐噪声，采用中值滤波可以很好的去除，用均值也可以取得一定的效果，但是会引起边缘的模糊。同时，中值滤波器对脉冲型噪声有很好的去除效果，因为脉冲点都是突变的点，排序以后输出中值，那么那些最大点和最小点就可以去掉了，但是中值滤波对高斯噪音效果较差。

中值滤波的做法是以处理窗内原图灰度值的“中值”作为“窗口”。以一维 5 点中值滤波为例，若原信号序列为“70,80,210,110,140”，即斜坡变化的中心处有大孤立噪声。做中值滤波时，取 5 个数的中值“110”作为滤波后，原图“210”所在的中心位置处的新值。可见，不论孤立噪声有多大都可以被滤除。若噪声不是孤立的，而是连续两个相等的值出现，则仍可以用中值滤波完全滤除，但如果是三个取值相同的点连在一起，用中值滤波就无法完全滤除了。

二维中值滤波是以二维窗内像素灰度值的中值作为窗中心处的新值。常用的二维窗形状有十字形窗、×形窗和正方形窗。用正方形窗进行中值滤波时，也能在去除噪声的同时保持边缘，但常会出现“缺角”的情况，而十字形窗对 0 度、90 度线以及角点有保护作用，×形窗则对 45 度线和 135 度线以及角点具有保护作用。

在抑制图像噪声和保护细节两方面存在一定的矛盾：窗口滤波小，可较好地保护图像中某些细节，但滤除噪声的能力会受到限制；滤波窗口大，可加强噪声抑制能力，但对细节的保护能力会减弱，有时会滤去图像中的一些细线、尖锐边角等重要细节，从而破坏图像的几何结构。这种矛盾在图像中噪声干扰较大时表现得尤为明显。要精心选择处理窗的大小，尽量在去除噪声的同时又能保留图像中的细节点。

由于标准中值滤波去脉冲噪声的性能受滤波窗口尺寸的影响较大，为了解决这个问题，人们提出了自适应中值滤波方法。自适应中值滤波的基本思想是将图像分为几个子块，通过对各子块中的像素进行噪声检测，将其分为受噪声污染像素和未受污染像素两类；统计受污染像素的个数以确定子图像中噪声干扰大小，根据噪声干扰程度自适应地调整滤波窗口的尺寸；最后采用改进的中值滤波方法对子图像中的噪声点进行滤波处理。自适应中值滤波在很大程度上缓和了噪声抑制和保护细节之间的矛盾，对噪声干扰较大的图像去噪时也能取得良好的效果，较标准中值滤波具有更优良的滤波性能，为消除图像中的脉冲噪声提供了一种有效途径。

下面我们对一幅指纹图像进行中值滤波，去除图像中的椒盐噪声等。如图 2-9 所示，图(a)为原始灰度图像，其中有一些明显的噪声，图(b)为中值滤波后的图像，噪声得到了明显的滤除。

图 2-8　中值滤波对比图

2.3.2　高斯滤波器

高斯滤波是一种线性平滑滤波，适用于消除高斯噪声，广泛应用于图像处理的减噪过程，也是在指纹图像处理过程中使用最多的滤波器。通俗地讲，高斯滤波就是对整幅图像进行加权平均的过程，每一个像素点的值，都由其本身和邻域内的其它像素值经过加权平均后得到。

高斯滤波的具体操作是用一个模板(或称卷积、掩模)扫描图像中的每一个像素,用模板确定的邻域内像素的加权平均灰度值去替代模板中心像素点的值。

若使用 3×3 模板,则其计算公式为:

$$\begin{aligned}\boldsymbol{g}(x,y)=\{&\boldsymbol{f}(x-1,y-1)+\boldsymbol{f}(x-1,y+1)+\boldsymbol{f}(x+1,y-1)+\boldsymbol{f}(x+1,y+1)+\\&[\boldsymbol{f}(x-1,y)+\boldsymbol{f}(x,y-1)+\boldsymbol{f}(x+1,y)+\boldsymbol{f}(x,y+1)]\times 2+\boldsymbol{f}(x,y)\times 4\}/16\end{aligned} \tag{2-9}$$

式中,$\boldsymbol{f}(x,y)$ 为图像中(x,y)点的灰度值;$g(x,y)$为该点经过高斯滤波后的值。

一维高斯函数的计算公式为:

$$G(x)=\frac{1}{2\pi\sigma}\mathrm{e}^{-\frac{x^2}{2\sigma^2}} \tag{2-10}$$

对于图像处理来说,常用二维零均值离散高斯函数作平滑滤波器。二维高斯函数的计算公式为:

$$G(x,y)=\frac{1}{2\pi\sigma^2}\mathrm{e}^{-\frac{x^2+y^2}{2\sigma^2}} \tag{2-11}$$

理论上,高斯分布在所有定义域上都有非负值,这就需要一个无限大的卷积核。实际上,仅需要取均值周围 3 倍标准差内的值,以外部分直接去掉即可。如图 2-9 为一个标准差为 1.0 的整数值高斯核。

图像去噪就是压制图像的噪音部分。因此,如果噪音是高频,从频域的角度来看,就是需要用一个低通滤波器对图像进行处理。通过低通滤波器可以抑制图像的高频分量,高斯滤波被用作平滑滤波器的本质原因是因为它是一个低通滤波器(让某一频率以下的信号分量通过,而对该频率以上的信号分量大大抑制)。高斯滤波的输出是领域像素的加权平均,同时离中心越近的像素权重越高,滤波后图像被平滑的程度取决于高斯函数的标准差。因此,相对于均值滤波(mean filter),它的平滑效果更柔和,而且边缘保留的也更好。

$\frac{1}{273}$

1	4	7	4	1
4	16	26	16	4
7	26	41	26	7
4	16	26	16	4
1	4	7	4	1

图 2-9　高斯核

下面我们对一幅指纹图像进行高斯滤波,去除图像中的高斯噪声并平滑图像。如图 2-10 所示,图(a)为原始灰度图像,其中有一些明显的噪声,图(b)为高斯滤波后的图像,噪声得到了明显的滤除。

(a)　　(b)

图 2-10　高斯滤波对比图

2.4 图像中的形态学处理

形态学处理也是数字图像处理中一种常用的手段，在自动指纹识别系统中，它常被用于指纹分割后续处理及增强等环节中。数学形态学是以形态结构元素为基础对图像进行分析的数学工具。它的基本思想是用具有一定形态的结构元素去度量和提取图像中的对应形状，以达到对图像分析和识别的目的。它是一门建立在集论基础上的学科，是几何形态学分析和描述的有力工具。

数学形态学诞生于 1964 年，法国巴黎矿业学院博士生塞拉(J. Serra)和导师马瑟荣(G. Matheron)，在从事铁矿核的定量岩石学分析及预测其开采价值的研究中提出“击中/击不中变换”，并在理论层面上第一次引入了形态学的表达式，他们的工作奠定了这门学科的基础。他们在法国共同建立了 Fontainebleau 数学形态学研究中心。在以后的几年研究中，他们逐步建立并完善了数学形态学的理论体系。此后，又研究了基于数学形态学的图像处理系统。

1982 年塞拉(J. Serra)出版的专著“*Image Analysis and Mathematical Morphology*”是数学形态学发展的重要里程碑，表明数学形态学在理论上趋于完备在应用上不断深入。数学形态学已经构成一种新的图像处理方法和理论，成为计算机数字图像处理的一个重要研究领域，并且已经应用于多门学科的数字图像分析和处理过程中。这门学科在计算机文字识别、计算机显微图像分析、医学图像处理、图像编码压缩、工业检测、计算机视觉和汽车运动情况检测等方面都取得了非常成功的应用。另外，它在指纹检测、经济地理、音乐合成和断层 X 光照像等领域也已经发挥了重要的作用。

数学形态学的应用可以简化图像数据，保持它们基本的形状特征，并除去不相干的结构。在指纹图像处理中，可以利用形态学算法对二值图像进行边界提取、骨架提取、孔洞填充和角点提取等工作。数学形态学的基本运算有 4 个：膨胀、腐蚀、开启和闭合。它们在二值图像及灰度图像中各有特点，基于这些基本运算还可以推导和组合成各种数学形态学实用算法，下面我们将会分别详细介绍这些基本运算。

2.4.1 腐蚀与膨胀

腐蚀和膨胀两个操作是形态学处理的基础，许多形态学算法都是以这两种原始操作为基础的。

1. 腐蚀

作为 Z 中的集合 A 和集合 B，使用 B 对 A 进行腐蚀，用 $A \otimes B$ 表示，并定义为：

$$A \otimes B = \{z \mid (B)_z \subseteq A\} \tag{2-12}$$

该式是指当进行 z 平移后的 B，其点若全部包含在 A 中，这时，我们记下这个点 Z，所有满足上述条件的 Z 点集合称为 B 对 A 的腐蚀。腐蚀“收缩”或“细化”二值图像中的对象。腐蚀具体的过程如图 2-11 所示。

图 2-11 中 X 是被处理的对象，B 是结构元素。对于任意一个在阴影部分的点 a，X

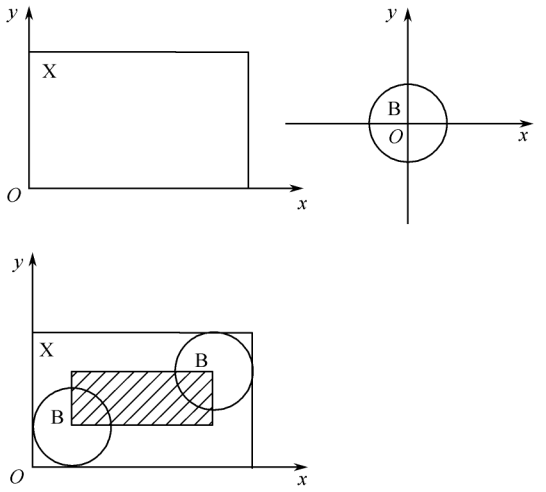


图 2-11　腐蚀的示意图

被 B 腐蚀的结果就是阴影部分。阴影部分在 X 的范围之内，且比 X 小，就像 X 被剥掉了一层似的，这就是称其为腐蚀的原因。

值得注意的是，上面的 B 是对称的，即 B 的对称集 $B^v=B$，所以 X 被 B 腐蚀的结果和 X 被 B^v 腐蚀的结果是一样的。如果 B 不是对称的，如图 2-12 所示，X 被 B 腐蚀的结果和 X 被 B^v 腐蚀的结果不同。

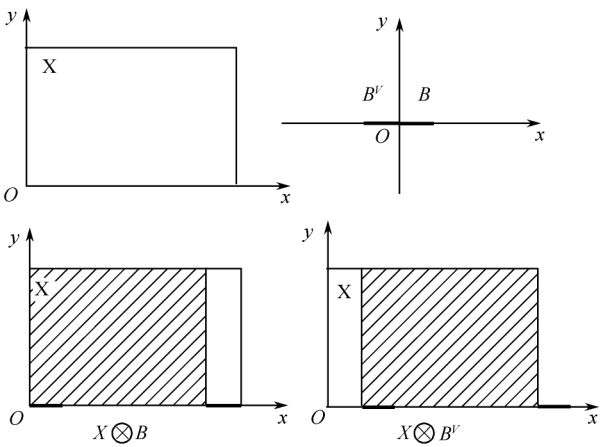


图 2-12　结构元素非对称时，腐蚀的结果不同

下面我们针对某一图像具体分析如何进行腐蚀运算，如图 2-13 所示。

在图 2-13 中，左边是被处理的图像 X(二值图像，我们针对的是黑点)，中间是结构元素 B，标有 origin 的点是中心点，即当前处理元素的位置，我们在介绍模板操作时也有过类似的概念。腐蚀的方法是，用 B 的中心点和 X 上的点逐一比对，如果 B 上的所有点都在 X 的范围内，则该点保留，否则将该点去掉；右边是腐蚀后的结果。可以看出，它仍在原来 X 的范围内，且比 X 包含的点要少，就像 X 被腐蚀掉了一层。

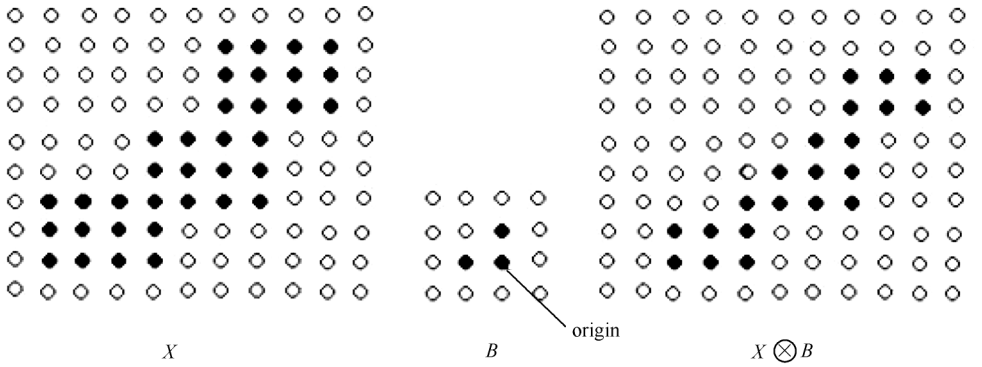


图 2-13　腐蚀运算

通过这个例子我们可以看出，腐蚀实际上是把图像的外围去掉，同时保留图像内部的部分

2. 膨胀

膨胀是数学形态学中除腐蚀之外的另一种基本运算。膨胀在数学形态学中的作用与腐蚀的作用正好相反，它是对二值化物体边界点进行扩充，将与物体接触的所有背景点合并到该物体中，使边界向外部扩张的过程。如果两个物体之间的距离比较近，则膨胀运算可能会把两个物体连通到一起，膨胀对填补图像分割后物体中的空洞很有用。A 和 B 是 Z^2 中的集合，B 对 A 的膨胀定义如式(2-13)所示：

$$A \oplus B = \{z \mid (\hat{B})_z \cap A \neq \varnothing\} \tag{2-13}$$

膨胀是在图像中“加长”或“变粗”的操作。这个公式是以 B 关于它的原点的映像，并且以 z 对映像进行平移为基础的。B 对 A 的膨胀是所有位移 z 的集合，这样，$\hat{B}$和 A 至少有一个元素是重叠的。膨胀的具体操作如图 2-14 所示。

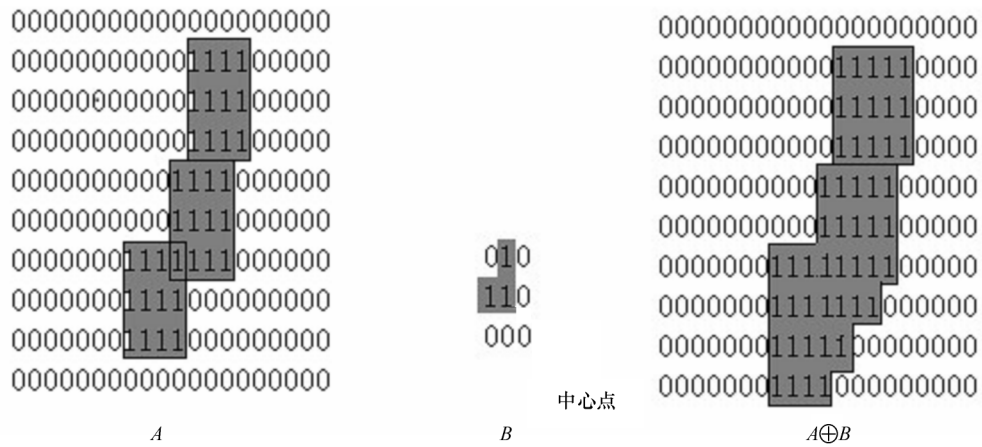
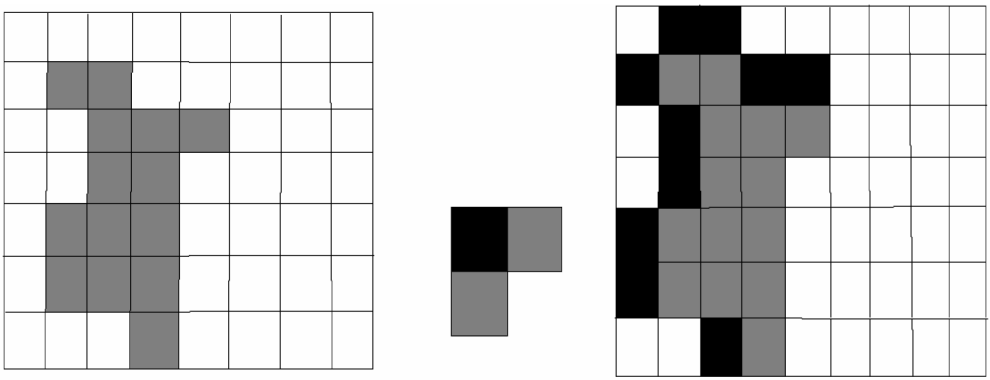


图 2-14　$A \oplus B$ 示意图

在图 2-14 中，左边是被处理的二值图像，针对的是“1”点，中间是结构元素 B。膨胀的方法是，用 B 的中心点和 A 上的点及 A 周围的点逐个比对，如果 B 上有一个“1”落在

A 的范围内，则该点就为“1”；右边是膨胀后的结果。可以看出，它包括 A 的所有范围，就像 A 膨胀了一圈似的。

如图 2-15 所示，用结构元素 B[如图 2-15(b)所示]对目标图像 A[如图 2-15(a)所示]进行膨胀运算并得到运算结果[如图 2-15(c)所示]的过程。



(a)原图　　(b)结构元素图　　(c)膨胀示意图

图 2-15　膨胀示意图

在图 2-15 中，图(a)中白色的部分代表背景，灰色的部分代表目标图像 A。图 (b)中黑色的方格代表结构元素的中心点，灰色的方格代表邻域。图(c)中灰色的部分表示原目标图像，黑色的部分表示膨胀出来的结果。在膨胀处理过程中，将结构元素在图像中移动，如果结构元素的邻域与目标图像 X 有部分重合，则保留图像中对应于中心点的像素点。

2.4.2　开运算与闭运算

开运算和闭运算是由腐蚀与膨胀不同的组合而形成的。

1. 开运算

上面我们介绍了腐蚀和膨胀，看上去好像是一对互逆的操作，实际上，这两种操作不具有互逆的关系。开运算和闭运算正是依据腐蚀和膨胀的不可逆性演变而来的。先腐蚀后膨胀的过程称为开运算。原图经过开运算后，能够去除孤立的小点、毛刺和小桥(即连通两块区域的小点)，消除小物体、平滑较大物体的边界，同时并不明显改变其面积。开运算的数学表达式如式(2-14)所示：

$$S=A\cdot B=(A\otimes B)\oplus B \tag{2-14}$$

式中，S 表示进行开运算后的二值图像集合；B 表示用来进行开运算的结构元素，结构元素内的每一个元素取值为 0 或 1，它可以组成任何一种形状的图形，在图形中有一个中心点；A 表示原图像经过二值化后的像素集合。此公式的含义是用 B 来开启 A 得到集合 S，S 是所有在集合结构上不小于结构元素 B 的部分的集合，也就是选出了 A 中的某些与 B 相匹配的点，而这些点则可以通过完全包含在 A 中的结构元素 B 的平移来得到。

如图 2-16 所示，左边是被处理的二值图像，针对的是 1 点，中间是结构元素 B，标有 1

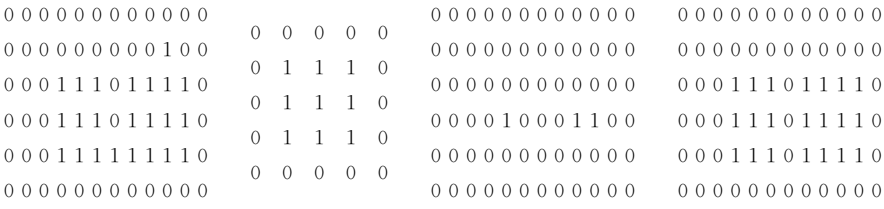


图 2-16　$(A\otimes B)\oplus B$

的点是中心点，即当前处理元素的位置，我们在介绍模板操作时也有过类似的概念。用 B 的中心点和 A 上的点逐一比对。对于腐蚀运算：如果 B 上的所有点都在 A 的范围内，则该点保留，否则将该点去掉。对于膨胀运算：如果 B 上有一个点落在 A 的范围内，则该点就为 1，否则，该点为 0。

可以看到，当使用圆盘结构元素时，开运算对边界进行了平滑，去掉凸角。在凸角点周围，图像的集合结构无法容纳给定圆盘，从而使凸角点被开运算删除。而当使用线段结构元素沿线段宽度方向较大的部分才能够保存下来。而较小的凸部分将被删除。因此，经过开运算后，能够去除孤立的小点，毛刺和小桥，平滑较大物体的边界，同时并不明显改变其面积。

2. 闭运算

闭运算是通过对腐蚀和膨胀的另一种不同次序的执行而得到的，闭运算是先膨胀后腐蚀的过程，其功能是用来填充物体内细小空洞、连接邻近物体、平滑其边界，同时不明显改变其面积。开运算的数学表达式如式(2-15)所示：

$$S=A\cdot B=(A\oplus B)\otimes B \tag{2-15}$$

式中，S 表示进行闭运算后的二值图像集合；B 表示用来进行闭运算的结构元素，结构元素内的每一个元素取值为 0 或 1，它可以组成任何一种形状的图形，在图形中有一个中心点；A 表示原图像经过二值化后的像素集合。此公式的含义是用 B 来闭合 A 得到的集合 S，就是图像 A 与经过映射和平移的结构元素 B 的交集不为空的点的集合。

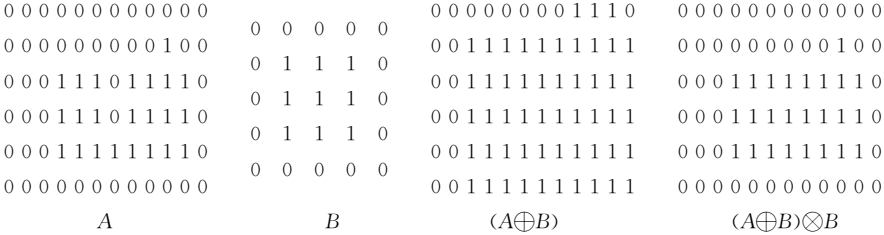


图 2-17　$(A\oplus B)\otimes B$

如图 2-17 所示，左边是被处理的二值图像，针对的是 1 点，右边是结构元素 B，可以看到原图经过闭运算后，断裂的地方被弥合了。

下面是使用不同形态学操作对指纹图像进行处理的效果图。在图 2-18 中，图(a)为原图像，图(b)为开操作的腐蚀阶段图像，图(c)为开操作的膨胀阶段图像，图(d)为闭操作

的膨胀阶段图像，图(e)为闭操作的腐蚀阶段图像。

(a)　(b)　(c)

(d)　(e)

图 2-18　使用不同形态学操作对指纹图像进行处理的效果图

2.5　边缘检测

数字图像处理可以看作是为了实现某一任务从包含有大量的不相关的信息中抽出对我们有用的信息的过程。同样的，在自动指纹识别系统中，我们需要扔掉一些不必要的信息，尽可能利用指纹图像中不变的性质来达到识别的效果。而边缘就是一种重要的不变性质，光线的变化显著地影响了一个区域的外观，但是不会改变它的边缘，边缘是图像的基本特征。

所谓边缘，是指图像中灰度发生急剧变化的区域，或者说是指周围像素灰度有阶跃变化或屋顶变化的那些像素的集合。边缘检测是图像处理中的重要内容，目的是在有噪声背景的图像中确定出目标物边界的位置。边缘虽然不一定对应图像中物体的边界，但是边缘具有十分令人满意的性质，它能大大地减少要处理的信息同时又保留了图像中物体的形状信息。

边缘检测的实质是采用某种算法来提取图像中对象与背景间的交界线。我们将边缘定义为图像中灰度发生急剧变化的区域边界。图像灰度的变化情况可以用图像灰度分布的梯度来反映，因此我们可以用局部图像微分技术来获得边缘检测算子。经典的边缘检测方法，是对原始图像中像素的某个邻域来构造边缘检测算子，其过程如图 2-19 所示。

首先通过平滑来滤除图像中的噪声，然后进行一阶或二阶微分运算，求得梯度最大值或二阶导数的过零点，最后选取适当的阈值来提取边界。经典的边缘检测方法有一阶微分边缘检测方法、差分边缘检测算法、Sobel 算子边缘检测的方法等，下面我们分别详细介绍这几种方法。

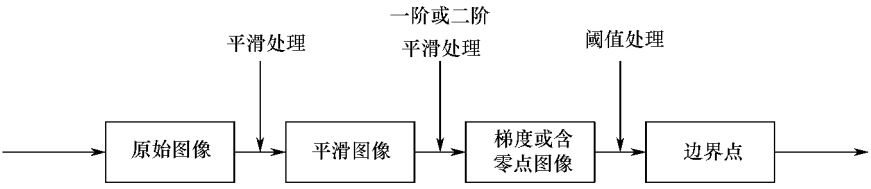


图 2-19　图像边缘检测的过程

2.5.1　一阶微分边缘检测

图像的局部边缘定义为两个强度明显不同的区域之间的过渡，图像的梯度函数，即图像灰度变化的速率将在这些过渡边界上存在最大值。早期的边缘检测是通过基于梯度算子或一阶导数的检测器来估计图像灰度变化的梯度方向，增强图像中的这些变化区域，然后对该梯度进行阈值运算，如果梯度值大于某个给定门限，则存在边缘。

一阶微分是图像边缘和线条检测最基本的方法。目前应用比较多的也是基于微分的边缘检测算法。图像函数 $\boldsymbol{f}(x,y)$ 在点(x,y)的梯度(即一阶微分)是一个具有大小和方向的矢量，如式(2-16)所示：

$$\nabla \boldsymbol{f}(x,y)=[G_x,G_y]^{\mathrm{T}}=\left[\frac{\partial f}{\partial x},\frac{\partial f}{\partial y}\right]^{\mathrm{T}} \tag{2-16}$$

$\nabla f(x,y)$的幅度为：

$$\mathrm{mag}(\nabla f)=g(x,y)=\sqrt{\frac{\partial^2 f}{\partial x^2}+\frac{\partial^2 f}{\partial y^2}} \tag{2-17}$$

方向角的公式为：

$$\phi(x,y)=\arctan\left|\frac{\partial f}{\partial y}\Big/\frac{\partial f}{\partial x}\right| \tag{2-18}$$

以上述理论为依据，人们提出了许多算法，常用的方法有：差分边缘检测、Roberts 边缘检测算子、Sobel 边缘检测算子、Prewitt 边缘检测算子、Kirsch 算子、Robinson 边缘检测算子、Laplace 边缘检测算子等。

所有的基于梯度的边缘检测器之间的根本区别有三点：

(1) 算子应用的方向。

(2) 在这些方向上逼近图像一维导数的方式。

(3) 将这些近似值合成梯度幅值的方式。

2.5.2　差分边缘检测

当我们处理数字图像的离散域时，可用图像的一阶差分代替图像函数的导数。二维离散图像函数在 x 方向上的一阶差分定义为：

$$f(x+1,y)-f(x,y) \tag{2-19}$$

$$f(x,y+1)-f(x,y) \tag{2-20}$$

利用像素灰度的一阶导数算子在灰度迅速变化处得到极值来进行奇异点的检测。它在某一点的值就代表该点的“边缘强度”，可以通过对这些值设置阈值来进一步得到边缘图像。但是用差分检测边缘必须使差分的方向与边缘方向垂直，这就需要对图像的不同方向都进行差分运算，增加了实际运算的繁琐性。差分边缘检测一般为垂直边缘检测、水平边缘检测、对角线边缘检测，如图 2-20 所示。

$$\begin{bmatrix} 0 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

(a) 垂直边缘　(b)水平边缘　(c)对角线边缘

图 2-20　三种差分边缘检测

差分边缘检测方法是最原始、基本的方法。根据灰度迅速变化处一阶导数达到最大(阶跃边缘情况)原理，利用导数算子检测边缘。这种算子具有方向性，要求差分方向与边缘方向垂直，运算繁琐，目前很少采用。

2.5.3　Sobel 算子

Sobel 提出一种将方向差分运算与局部平均相结合的方法，即 Sobel 算子。该算子是以 $f(x,y)$为中心的 3×3 邻域上计算 x 和 y 方向的偏导数，如式(2-21)所示：

$$\begin{cases} \boldsymbol{s}_x=\{\boldsymbol{f}(x+1,y-1)+2\boldsymbol{f}(x+1,y)+\boldsymbol{f}(x+1,y+1)\}- \\ \quad \{\boldsymbol{f}(x-1,y-1)+2\boldsymbol{f}(x-1,y)+\boldsymbol{f}(x-1)-(y+1)\} \\ \boldsymbol{s}_y=\{\boldsymbol{f}(x-1,y+1)+2\boldsymbol{f}(x,y+1)+\boldsymbol{f}(x+1)-(y+1)\}- \\ \{\boldsymbol{f}(x-1,y-1)+2\boldsymbol{f}(x,y-1)+\boldsymbol{f}(x+1,y-1)\} \end{cases} \tag{2-21}$$

实际上，式(2-21)应用了 $\boldsymbol{f}(x,y)$邻域图像强度的加权平均差值。其梯度大小为

$$\boldsymbol{g}(x,y)=\sqrt{(\boldsymbol{s}_x^2+\boldsymbol{s}_y^2)} \tag{2-22}$$

或取绝对值：

$$\boldsymbol{g}(x,y)=|\boldsymbol{s}_x|+|\boldsymbol{s}_y| \tag{2-23}$$

Sobel 边缘检测算子方向模板如图 2-21 所示。

$$\begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix}$$

图 2-21　Sobel 边缘检测算子方向模板

由上面两个卷积算子对图像运算后，代入式(2-23)中，可求得图像的梯度幅度值 $\boldsymbol{g}(x,y)$，然后适当选取门限 TH，进行如下判断：$\boldsymbol{g}(x,y)>\mathrm{TH}$，$(i,j)$为阶跃状边缘点，$\{\boldsymbol{g}(i,j)\}$为一个二值图像，也就是图像的边缘图像。

Sobel 算子很容易在空间实现，Sobel 边缘检测器不但能产生较好的边缘检测效果，同时，因为 Sobel 算子引入了局部平均，使其受噪声的影响也比较小。当使用大的邻域时，抗噪声特性会更好，但这样做会增加计算量，并且得到的边缘也较粗。当对精度要求不是很高时，Sobel 是一种较常用的边缘检测方法。

在自动指纹识别系统中，Sobel 算子发挥了重要作用，在指纹增强步骤中，我们利用 Sobel 算子求取方向场，具体的计算方法和相关结果请参见第 8 章。

2.6 本章小结

围绕学习自动指纹识别系统所需要了解的数字图像基础知识和基本方法，本章从以下几个方面介绍了数字图像处理的基础知识：首先，解释清楚了什么是数字图像、灰度图像以及图像质量的评估。其次，针对指纹图像处理中常用的变换方法和滤波方法，重点介绍了傅里叶变换、霍夫变换、中值滤波以及高斯滤波的相关知识。最后，我们详细介绍了指纹图像处理中的涉及的形态学处理方法和边缘检测算法。本章所介绍的基础知识和基本方法主要服务于本书中涉及的指纹识别处理方法中的数字图像处理知识，如有遗漏之处，请查阅数字图像处理的其它相关资料。

习题与思考题

1. 结合自动指纹识别系统中使用的指纹图像，分析说明数字图像的优点与意义。
2. 给出一幅灰度指纹图像，阐述这幅图像中大小，位深的概念，并解释其灰度矩阵的具体含义。
3. 结合生活中的实际例子，谈谈图像质量评估的具体应用和价值。
4. 数字图像处理系统由哪几部分组成，并举一个生活中使用数字图像处理系统的应用场景。
5. 解释傅里叶变换的具体原理并利用 Matlab 软件实现一幅图像的快速傅里叶变化。
6. 说明中值滤波的含义原理，利用 Matlab 软件建立一个 3×3 的模板，实现对某一灰度图像的中值滤波操作。
7. 对一幅含有较多噪声的图像进行高斯低通滤波处理，对比滤波前后的变化，观察滤波效果。
8. 解释数学形态学中的开、闭运算与腐蚀、膨胀操作之间的关系。
9. 反复进行图像腐蚀操作的限制作用是什么？假设不使用通常(一个点)的结构元素。
10. 利用差分边缘检测算法和 Sobel 算子分别对某一图像进行边缘检测，结合结果分析这两种算法处理的优缺点。

第 3 章　认识指纹图像

生物特征包括指纹、人脸、虹膜、视网膜、语音、掌形、签名和步态等。采取任何一种或几种生物特征作为自动识别系统的识别特征，都需要对所选取的特征进行数字化。指纹作为最为广泛使用的生物特征，在实际使用时仍需要转化为数字化指纹图像，这样才能更利于整个识别过程的自动化处理。

数字指纹图像具有独特的结构和特征，正是由于这些结构和特征才使得数字指纹图像具有分辨不同人的功能。因此，在掌握数字图像处理的基本知识之后，准确地了解数字指纹图像才能更好地发挥数字指纹图像的识别功能。

本章的内容 3.1 节介绍指纹图像的形成和采集方法，3.2 节介绍指纹图像的描述，3.3 节详细介绍了二级特征中的脊线特征，3.4 节总结了本章的内容。

3.1　指纹图像概述

指纹是每个人都具有的生物特征，只有极少数人因基因突变或罹患特殊疾病而天生没有指纹，如图 3-1 所示，其中方框中为没有指纹的指尖。

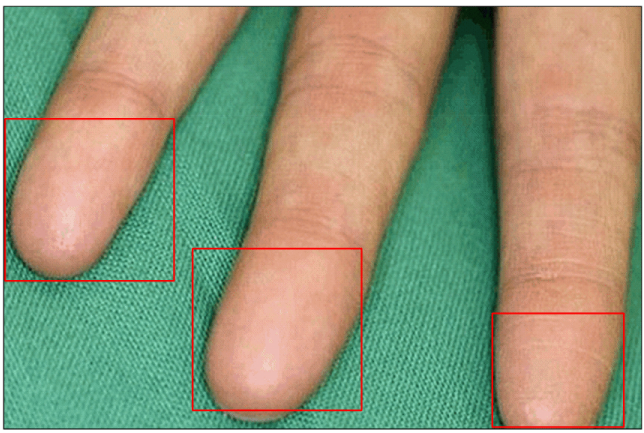


图 3-1　天生无指纹人的手指

除了天生无指纹的人之外，正常人的指纹在遭受物理烧伤或化学烧伤后，指纹也可能会遭到严重损坏，这时他们也无法通过指纹进行身份验证。下面就正常人指纹的形成及采集展开介绍。

指纹在胎儿第三、四个月便开始产生，到第六个月左右就形成了，当婴儿长大成人，指纹也只不过放大增粗，它的纹样不变。在皮肤发育过程中，虽然表皮、真皮以及基质层都在共同成长，但柔软的皮下组织长得比相对坚硬的表皮快，因此会对表皮产生源源不断的上顶压力，迫使长得较慢的表皮向内层收缩塌陷，逐渐变弯打皱，以减轻皮下组织施加给它的压力。如此一来，一方面使劲向上攻，一方面被迫往下撤，导致表皮长得弯弯曲曲，坑

洼不平，形成纹路。这种变弯打皱的过程随着内层组织产生的上层压力的变化而波动起伏，形成凹凸不平的脊纹或褶皱，直至发育过程终止，最终定型为至死不变的指纹。

一岁左右婴儿的指纹比成人指纹通常要轻、浅。如图 3-2 所示，对比可看出两岁婴儿的指纹明显比一岁婴儿的指纹清晰。

（a）一岁婴儿的指纹图像　　（b）两岁婴儿的指纹图像

图 3-2　婴儿的指纹图像

成人的指纹会在成长过程中受到磨损、割伤等伤害，使得指纹图像产生伤痕，如图 3-3 所示，在图中右下方的方框内是割伤产生的伤痕，可以看到这个伤痕将连续的纹线断开。

图 3-3　带有伤痕的成人指纹图像

指纹图像可以通过物理方法和化学方法来获取。物理方法包括粉末法、磁粉法等。化学法包括碘熏法、宁海得林(Ninhydrin)法、硝酸银法和荧光试剂法等。除此之外，指纹图像还可以使用采集仪器进行采集。使用不同的指纹采集仪或采集者施加不同的压力都会对采集的指纹图像产生影响。关于采集的详细内容可以参见本书第 6 章。

虽然指纹只是人类身体的一小部分，但它所含的信息中可用于身份识别的信息量相当大。只有掌握指纹图像中所蕴含的信息，才能建立更为完善、精确的指纹自动识别系统。下面内容详细介绍指纹中包含的信息。

3.2　指纹图像描述

指纹图像是指尖表皮外部表现的复制，手指上的许多伤口如表皮割伤、磨伤或切伤不会影响到内在的脊线结构，而且原来的指纹模式可以从长出来的任何新皮肤上复制而得。了解了指纹图像的定义之后，下面对指纹图像上的信息进行详细的介绍。

指纹图像中的信息是通过特征来表示的，所有特征可以分为一级特征、二级特征和三级特征。一级特征是指纹的全局脊线流形；二级特征是细节特征；三级特征是包含气孔、纹线边缘、疤痕、细点线、汗孔等更加细节的特征信息。

一级特征(Level 1)包括脊线、谷线、纹线流向流、中心花纹、三角区、奇异区域、纹线类型和纹型。下面就每种一级特征进行详细介绍。

脊线(Ridge)和谷线(Valley) 属于指纹的一级特征。它们分别是灰度指纹图像中的较暗的线和较亮的线。

如图 3-4 所示(该图来源于 Fingerprint Verification Competition 2002DB1)，用白色圆点画出的为脊线，用黑色圆点画出的为谷线。整个指纹图像是由脊线和谷线构成的一个具有很强纹理性的结构，且这个结构具有一定的规律和特点。

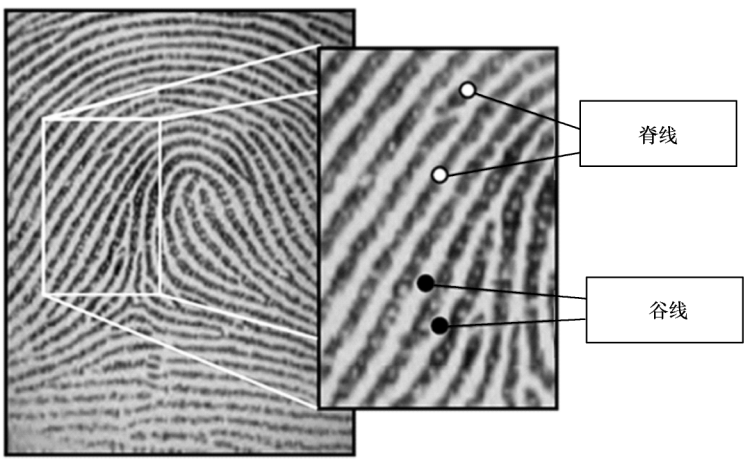
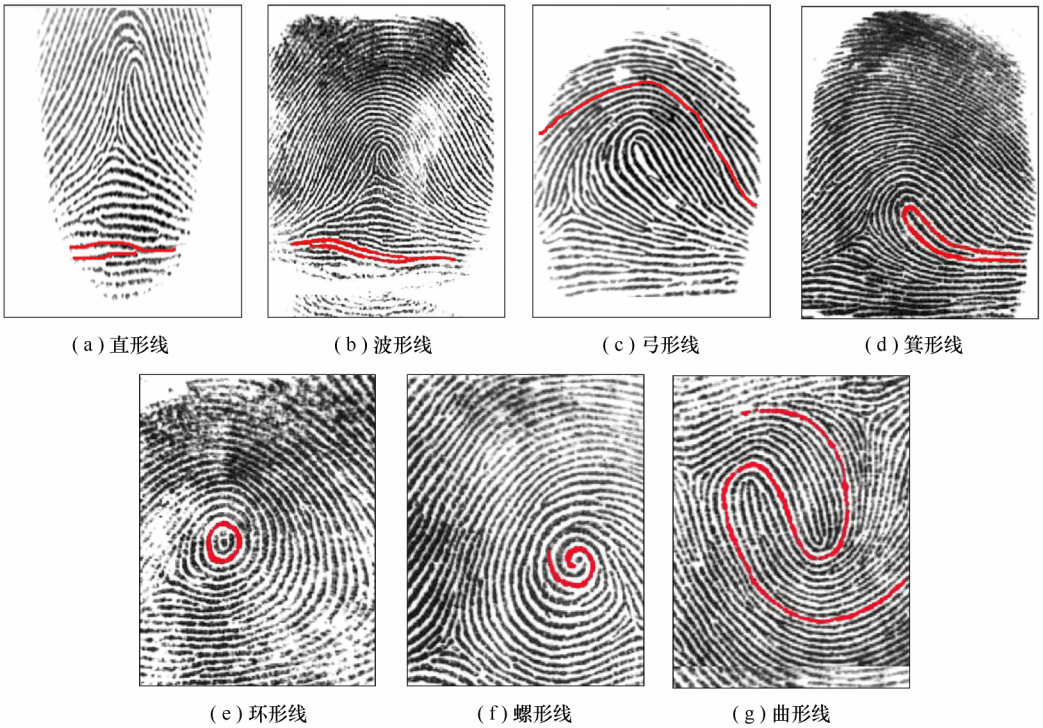


图 3-4　指纹图像中的脊线和谷线

在成人指纹图像中，脊线从窄到宽为 100～300μm，一个完整的脊谷线约为 500μm。

指纹的纹线属于一级特征，它是组成指纹的曲线，根据纹线的形状可以将纹线细分为

7 种类型：直形线，波浪线，弓形线，箕形线，环形线，螺形线和曲形线，如图 3-5 所示。



(a) 直形线　(b) 波形线　(c) 弓形线　(d) 箕形线

(e) 环形线　(f) 螺形线　(g) 曲形线

图 3-5　7 种脊线类型

纹线流向流、中心花纹和三角区属于一级特征如图 3-6 所示。

(a) 纹线流向流　(b) 中心花纹　(c) 三角区

图 3-6　指纹纹线类型

奇异区域(Singular Regions)是脊线中存在的一个或者多个与众不同的形状区域。它可以广泛地分为三个类型：环形、三角点和螺纹，如图 3-7 所示。

其中螺纹可以看作是两个环连接而成的。中心点(Core)是指纹模式区中位于充分弯曲脊线里曲率最大的特殊点，也称为内部终点。由于指纹模式的多样性，很难在所有指纹图像中准确的找出中心点，如不含环和螺纹的指纹就很难定义中心点。

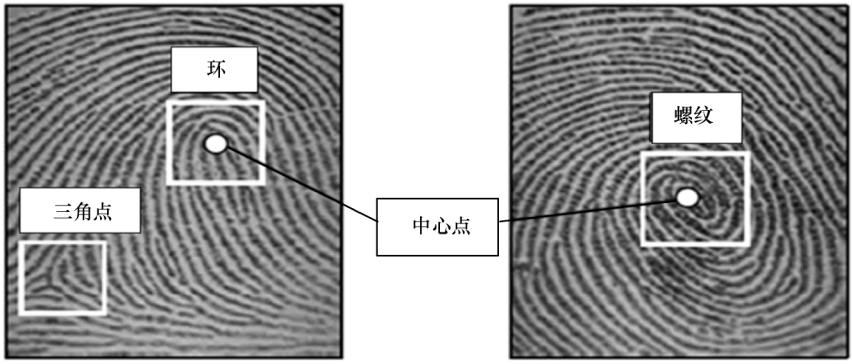


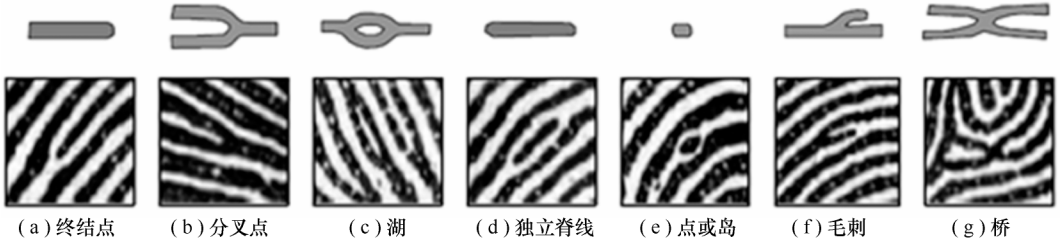
图 3-7　指纹图像中的奇异点

指纹纹型属于一级特征，它是指纹图像中由纹线构成的整幅图像的形状，包括弓形纹、箕形纹、斗形纹，如图 3-8 所示以及混杂型纹。

(a) 弓形纹　(b) 箕形纹　(c) 斗形纹

图 3-8　指纹纹型

二级特征(Level 2)主要是表示指纹中脊线不连续的多种形式的一些小的细节。比如，一个脊线突然中断(终结点)或者分成两条脊线(分叉点)。指纹细节点有多种类型：终结点、分叉点、湖、独立脊线、点或岛、毛刺和桥等，如图 3-9 所示。



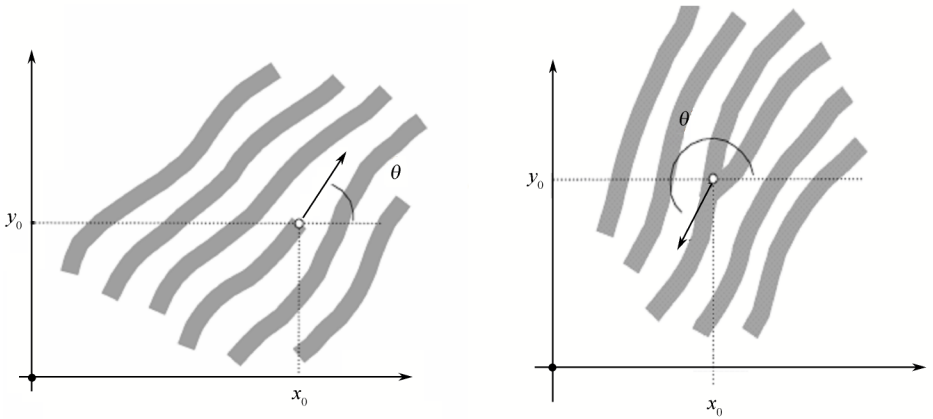
(a) 终结点　(b) 分叉点　(c) 湖　(d) 独立脊线　(e) 点或岛　(f) 毛刺　(g) 桥

图 3-9　7 种常见的细节点类型

指纹细节点常用于自动指纹匹配中，英国科学家 Francis Galton 是第一个对细节点进行分类的人，而且他毕生都在研究细节点。为了纪念他，所以细节点又称为“Galton 点”。

在一个全指纹中细节点个数一般多于 100 个。在瑞士洛桑大学 Christophe Champod 博士的论文“*Fingerprints and Other Ridge Skin Impressions*”和伊利诺伊大学 D. A. Stoney 博士的论文“*A systematic study of epidermal ridge minutiae*”中可以得到一些统计数据:在奇异区域内和奇异区域外的细节点密度分别为 0.49minutiae/mm^2 和 0.18minutiae/mm^2,即在奇异区域内和奇异区域外的细节点密度分别为每平方毫米平均有 0.49 个细节点和 0.18 个细节点。但是,一些细节点在空域和角频域的一致性或相关性就能够充分证明两个指纹图像来源于同一个手指。

细节点的位置可以用横纵坐标值和水平线与脊线的正切线之间的夹角来表示。具体如图 3-10(a)所示,该终结点的位置可以用(x_0,y_0)和 θ 表示。对图像[图 3-10(a)]取反,即图(a)中,像素值原为 255 的像素点转变为像素值为 0 的像素点,像素值为 0 的像素点转变为像素为 255 的像素点,这样,原图像[图 3-10(a)]中的脊线转变为谷线,谷线转变为脊线,分叉点变为了终结点,如图 3-10(b)所示。这样分叉点的坐标值也可以通过图 3-10(a)中方法求得。



(a)图中(x_0,y_0)是细节点坐标　　(b)对图(a)取反

图 3-10　细节点位置表示

脊线频率和脊线方向图都属于二级特征,它们分别是脊线在脊线上某一像素点的频率和方向。在实际应用中,这两个二级特征的使用较为频繁,且作用较为重要。因此,本章将单独介绍,具体内容请参见本章 3.3 节。

三级特征(Level 3)是使用高分辨率采集仪扫描指纹图像得到的特征。图 3-11 中展示了汗孔、纹线边缘、疤痕、细点线、皱纹、疣等的示意图。

其中最常用的三级特征为汗孔。表皮的每个脊线上都有汗孔。一般来说,汗孔分为两类,一类是关闭的,一类是打开的。关闭的汗孔分布在脊线上,打开的汗孔与谷线相交。在二值化后的指纹图像上,脊线比汗孔和谷线暗,汗孔和谷线比脊线亮,汗孔大小为 60～250μm。如图 3-12 所示。

每厘米的脊线上大约有 9～18 个汗孔。已经有数据证实 20～40 个汗孔就足够决定这个指纹所属的人。

以上为三种级别的特征的基本概念,下面将讲述三种级别的特征在指纹识别过程中

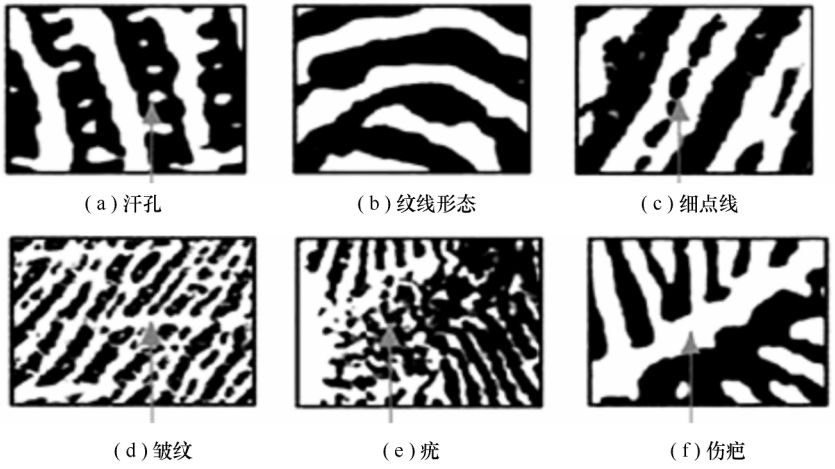


图 3-11　指纹图像中的三级特征

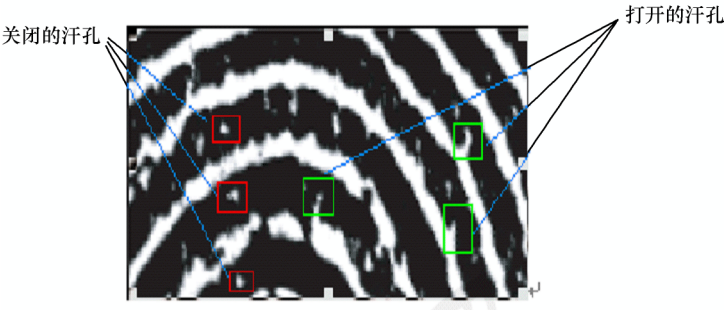


图 3-12　部分高精度指纹图像中的汗孔

的具体应用。

一级特征虽然不具有唯一性，但它可以作为指纹图像分类和检索的依据。

随着指纹在各方面的广泛应用，指纹数据库也随之而增大，这为后期的指纹比对过程增加了困难。为了减少搜寻时间，提高检索效率，需要建立某种索引机制来减少指纹比对所需要遍历的指纹数量。为此，人们根据指纹图像一级特征中的纹型特征对指纹的分类进行了以下探索。

1823 年，德国布雷斯劳大学(Breslau University)的捷克解剖学家 Jan Evangelista Purkynje 在论文“*Commentatio de examine physiologico organiwisus* (*Habilitatio inauguralis*)”中首次将指纹纹型分成了 9 类，如图 3-13 所示。

1899 年，Edward Henry 和他的两个助手建立了第一套指纹分类体系——亨利系统(Henry System)。该体系把人类指纹分为三大类，20 多个子类。后来美国联邦调查局在该体系的基础上，将人类指纹分为 8 个类型。但是在这 8 种指纹类型中，部分类型之间的差别较小，很难用计算机程序将它们准确地区分开来。因此，自动指纹分类算法中一般将这 8 种类型合并为图 3-14 中所示的 5 种类型。这 5 种类型分别为左旋[如图 3-14(a)所示]、右旋[如图 3-14(b)所示]、螺旋[如图 3-14(c)所示]、拱[如图 3-14(d)所示]和尖拱

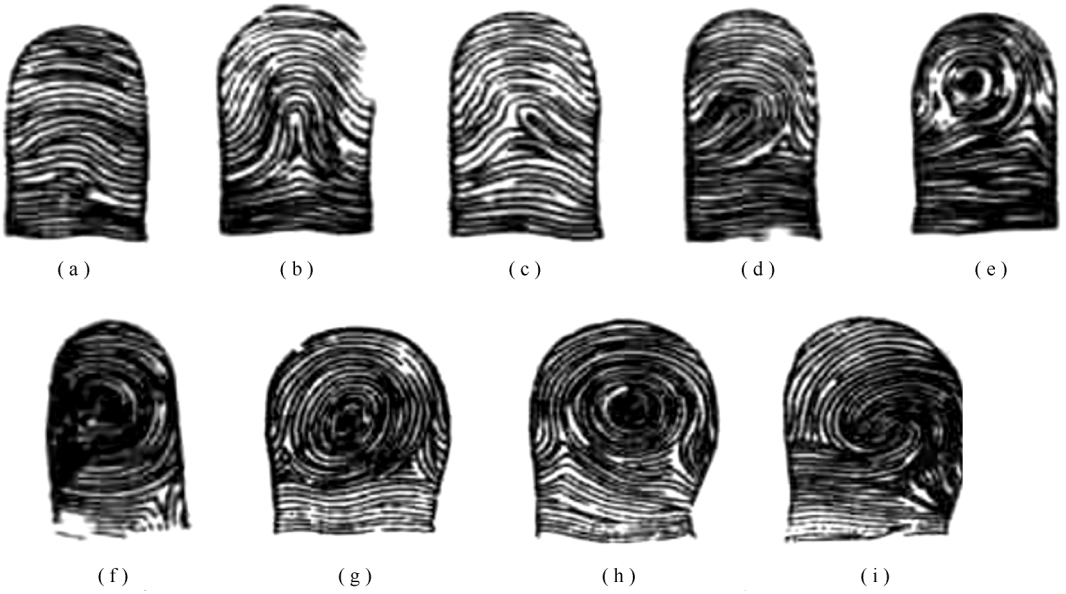


图 3-13　Purkynje 文章中列出的 9 种模式

[如图 3-14(e)所示]。有时还将拱和尖拱合并为一类,使之变成 4 种基本指纹类型。

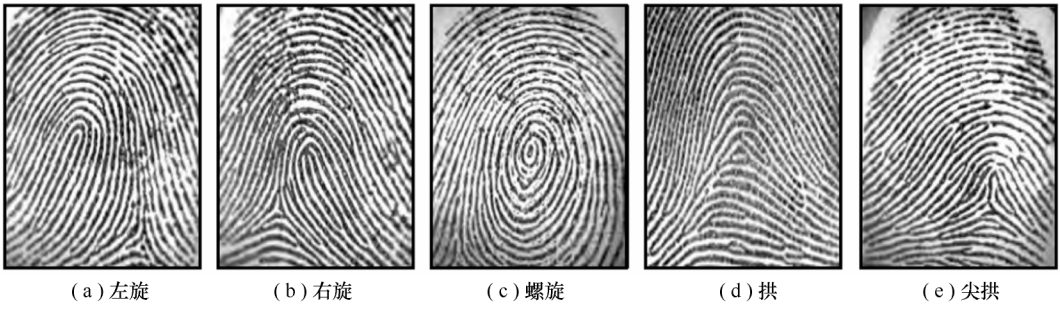


图 3-14　基本的 5 种纹线类型

二级特征种类繁多,具有相当强的个人身份证明力。

中心点在指纹匹配中可以作为标志进行预匹配,其它细节点类型在指纹匹配中作为判断两幅指纹图像是否匹配的依据。

由于细节点类型较多,实际应用中并不是每种都用来进行指纹匹配。在高精度的自动识别系统中仍然采取的是一种较为粗糙的细节点分类。如美国国家标准协会(American National Standards Institute,ANSI)在 2007 年提出了一种基于终结点、分叉点、复合点(三叉点或交叉点)和待定类型点的细节点分类方法,而 2004 年 FBI 的细节点分类中只使用了终结点和分叉点。

三级特征很有特色而且对进一步提升指纹识别的精确度,但是目前很少有自动指纹匹配技术采用三级特征,因为它们的可靠检测是以高分辨率(比如 1000 Dots Per Inch,

DPI)的扫描仪和高质量的指纹图像为基础。

指纹图像的信息中,一级特征可以用于指纹图像的分类,减少指纹比对次数和检索时间。三级特征可以用于需要较高可靠性的检测中。而在自动指纹识别系统中一般使用二级特征作为指纹匹配的标志,其中脊线特征作为二级特征中的重要组成部分,在指纹图像增强和匹配中都有很大的作用。因此,在下节中详细地对脊线特征进行介绍。

3.3　指纹的脊线特征

指纹的脊线特征属于指纹图像的二级特征,它包括脊线方向和脊线频率,代表了指纹的纹理性与方向性,携带了指纹图像中最重要的信息。

在指纹匹配中,大部分算法是根据细节点信息进行匹配的,但是图像中有效细节点的数量受到图像大小和质量等因素的影响,具有一定的局限性。脊线信息在指纹图像中较为丰富,可以引入脊线特征,与细节点信息相互补充,提高细节点匹配的准确性和自动指纹识别系统的可靠性。

3.3.1　指纹的脊线方向

脊线方向(Ridge Orientation)是指纹中某个像素点的局部脊线方向。像素点(x,y)处的局部脊线方向用角θ_{xy}来表示,角θ_{xy}为脊线穿过一个任意小的以像素点(x,y)为中心的邻域,与水平轴形成的夹角。如图 3-15 所示,它是一个值域为$[0,180)$的不确定方向的角。

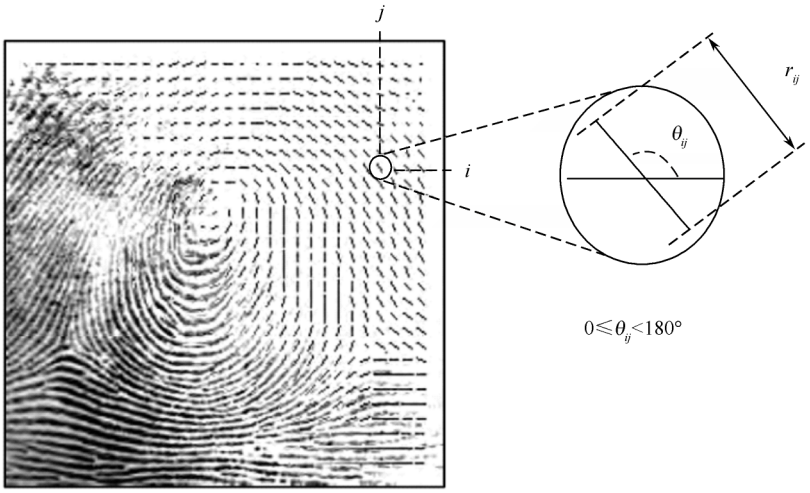


图 3-15　指纹图像 16×16 像素块中一个像素的局部脊线方向

在大多数指纹处理和特征提取算法中,并不是对每个像素计算其局部脊线方向,而是在离散位置计算其局部脊线方向。这样不仅能够减少计算量,而且它仍能通过插值法来获得在其它像素的局部脊线方向。

指纹方向图(Orientation Image)分为两类,一类是点方向图,描述了指纹每个像素点所在的脊线或谷线在该点的切线方向;另一类是块方向图,描述了在某一个小区域内指纹整体的方向,能够表现指纹在这一小块区域内脊线的走向。点方向图和块方向图都是指纹图像的重要特征,也为后续的分割,增强等操作提供了重要的操作依据。

方向图提取的基本思想是在原始灰度指纹图中计算每一个像素点或者每一块在各个方向上的某一个统计量(如灰度差、梯度等),根据这些统计量在各个方向上的差异,确定该像素点或者该分块的方向。对于某一个像素点来说,由于受到各种噪声的影响,可能会产生较大的随机误差,然而,对某一个具体的指纹来说,某一个小区域的方向总是近似一致的,因此利用块方向图来代替该区域中所有像素点的方向是可行的,而且可以有效地消除点方向图中的随机误差。因此在实际应用中往往采用块方向图,因为块方向图不但具有更强的抗噪性,而且块方向图的计算量要小于点方向图。块方向图可以在点方向图的基础上求得,也可以用其它算法直接求得,具体求法可参见本书第 8 章。

3.3.2 指纹的脊线频率

点(x,y)的脊线频率(Ridge Frequency)loy 是沿着一个假设的以(x,y)为中心的单位分割长度里脊线的数量。它与局部脊线方向 θ_{xy} 正交。频率图和方向图相似,可以在频率是离散的情况下进行定义,而且能够用矩阵表示。

在指纹图像的局部非奇异区域里,沿着垂直于脊线方向,指纹的脊线和谷线像素点值大致构成了一个二维的正弦波,如图 3-16 所示,图(a)中虚线表示灰度为图(b)中 x 轴值的一列的像素点。图(b)中的 x 轴存在 5 个波峰;连续波峰之间的 4 个距离的平均值决定了局部脊线频率。

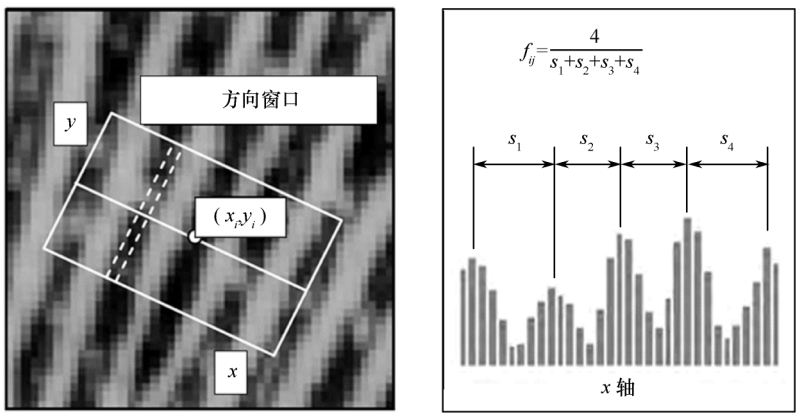


图 3-16 以(x_i,y_j)点为中心的方向窗

因此,指纹的脊线和谷线具有很好的局部频率特征。同样,求取这些互不重叠的局部区域的频率值,按各区域位置组成一个场结构,称之为指纹的频率场。

1998 年,密歇根州立大学(Michigan State University,MSU)的 A. K. Jain 教授通过

计算沿着局部脊线方向的两个连续顶点之间像素的平均数来估计局部脊线频率。

在(x_i, y_j)处的频率可以通过以下步骤计算得到：

(1) 在坐标系中定义一个以(x_i, y_j)为中心 32×16 的方向窗。

(2) 对每一列 x,求它在方向窗中对应像素的灰度水平的累加平均。这种平均可以使灰度水平更加光滑而且能够阻止脊线峰值由于脊线断点和气孔变模糊。

(3) f_{ij}定义为 x 轴上两个连续峰值间平均距离的倒数。

这种方法利用了在指纹图像质量较好的情况下,在垂直脊线方向上,脊线和谷线呈现离散正弦波形的特征来计算脊线频率。该算法认为正弦波形中波峰与波峰之间的距离就是脊线之间的距离,而脊线频率即为脊线距离的倒数。该算法虽然简单又快速,但是,实际的指纹图像特别是低质量指纹图像,在脊线方向上的投影波形往往不是很好的正弦波形,因此计算出的脊线频率误差较大。

针对上面算法的缺点,可以采用内插值法和低通滤波器法,还可以利用基于一阶和二阶导数的合适方法从 x 轴上提取脊线距离,具体内容可以参考 Davide Maltoni 等人于 2009 年出版的"*Handbook of Fingerprint Recognition Second Edition*"一书。

本节介绍了脊线特征中在某一像素点求取脊线方向和脊线频率的经典方法。掌握了某一像素点的脊线方向和频率之后,可以将整幅指纹图像的脊线方向和频率求出,形成指纹图像的方向图和频率图。将方向图和频率图用于指纹增强过程中可以使指纹的前景区域更为清晰。

3.4　本章小结

本章首先介绍了指纹图像的形成过程并对比了婴儿和成人的指纹图像,然后详细介绍了指纹图像中的三种级别的特征及其应用,最后对指纹图像二级特征中的脊线特征进行了详细介绍。

在自动指纹识别系统中,根据细节点信息可以对指纹图像进行比对。但细节点信息受到图像质量和图像大小的影响,因此,细节点信息和纹理特征相结合才能提高识别系统的准确性和效率。

习题与思考题

1. 如图 3-17 所示,基于本书中介绍的五种基本纹线类型,判断图中各指纹图像的指纹类型。
2. 如图 3-18 所示,写出每幅图包含的细节点类型,每种细节点类型找出至少一处。
3. 认真观察图 3-17 和图 3-18 中的图像,从指纹纹型、指纹所含纹线类型和指纹清晰度等方面说出其不同之处和相似之处。
4. 思考是否可以单独使用脊线特征作为准确识别一个人的依据？为什么？

图 3-17

图 3-18

第 4 章　自动指纹识别系统与加密系统

自动指纹识别系统(Automatic Fingerprint Identification System,简称 AFIS)是通过专门的指纹采集设备进行指纹图像的采集,对采集到的指纹图像进行预处理,然后对预处理后的指纹图像进行特征提取获得指纹的特征数据,最后与预先保存在指纹库中的指纹特征进行比对匹配,判断两个指纹是否来自于同一个手指,实现快速准确的身份认证的系统。

生物特征加密系统就是将生物特征技术与密码技术相结合,把提取到的生物特征与密钥绑定,用验证的生物特征对密钥进行解绑,应用解绑后的密钥进行加密解密的系统。

本章内容:4.1 节介绍自动指纹识别系统与加密系统的流程框架,4.2 节介绍指纹图像的采集,4.3 节介绍指纹图像的预处理,4.4 节介绍指纹图像的特征提取,4.5 节介绍指纹图像的匹配,4.6 节介绍生物特征加密系统,4.7 节总结本章的内容。

4.1　自动指纹识别系统与加密系统框架

自动指纹识别系统的组成主要包括指纹图像采集、指纹图像预处理、特征提取和指纹匹配 4 个部分,如图 4-1 所示。其中预处理又包括指纹图像的分割、增强和二值化等组成部分。

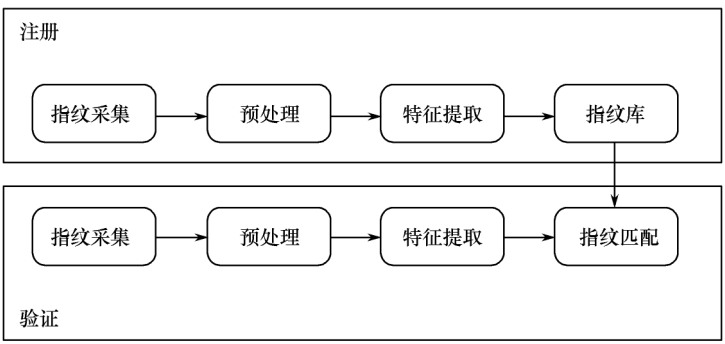


图 4-1　自动指纹识别系统

生物特征加密系统主要包括注册生物特征的获取,密钥和生物特征进行绑定,待验证的生物特征的获取,应用待验证的生物特征对密钥进行解绑,应用解绑后的密钥对信息进行加密解密几个组成部分,如图 4-2 所示。

如果将指纹特征应用于生物特征加密系统,那么生物特征加密系统中注册特征的获取部分就用到了自动指纹识别系统中的注册部分,待验证的生物特征的获取和应用待验

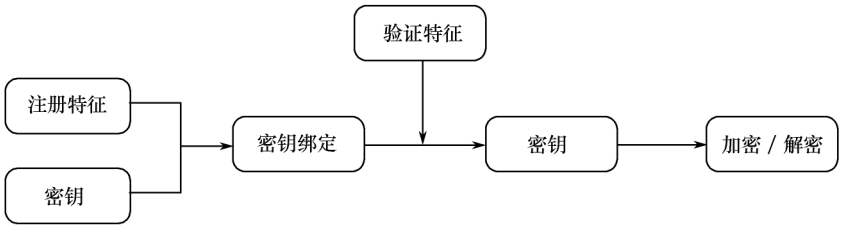


图 4-2　生物特征加密系统

证的生物特征对密钥进行解绑部分就用到了自动指纹识别系统中的验证部分。由此可见,自动指纹识别系统是应用指纹特征的生物特征加密系统的基础。

4.2　指纹图像的采集

指纹图像的采集是获取数字指纹图像的过程,也是自动指纹识别系统的第一步。因为采集到的指纹图像的质量好坏直接影响到指纹的识别结果,所以,指纹图像的采集也是自动指纹识别系统中不可忽视的重要组成部分。采集到的指纹图像如图 4-3 所示。

(a)　　(b)

图 4-3　FVC2002 指纹库中的指纹图像:(a)、(b)为 FVC2002 中同一手指的两幅指纹图像

由于指纹采集的面积较小,手指表面的干净程度也会影响采集到的指纹图像的质量,因此如何获取高质量的指纹图像是提高自动指纹识别系统性能的首要解决的问题。

早期指纹图像的获取是通过将蘸有黑色墨水的手指按在白色的纸上,留下一个黑白的指纹图像,然后通过扫描仪进行扫描得到数字的指纹图像。现在指纹图像的采集主要通过指纹传感器。指纹传感器可以分为光学指纹传感器、半导体指纹传感器和超声波指纹传感器。其中光学指纹传感器和半导体指纹传感器是现在应用最多的指纹传感器,如图 4-4 所示。本书将在第 6 章对指纹图像的采集技术进行详细地介绍。

(a) 光学指纹传感器　　(b) 半导体指纹传感器

图 4-4　指纹传感器

4.3　指纹图像的预处理

指纹图像的预处理就是对采集到的指纹图像进行前景区域分割、增强、二值化等处理的过程。通过指纹的预处理可以去除指纹图像中的干扰因素，保留图像的真实细节特征，使得指纹图像变得清晰，从而可以进行指纹特征的提取。

在实际的自动指纹识别系统中，由于手指表面与采集设备表面的非均匀接触、采集仪工作环境参数设置和手指表面的油脂、汗液、污渍、破皮都会使得采集到的指纹图像的质量不够理想，图像中含有大量的噪声。指纹图像中噪声的存在会很大程度上影响指纹特征提取的准确性，进而影响了指纹的匹配精度。为了能准确地提取指纹的特征，提高指纹的匹配精度，我们就需要对指纹传感器采集到的图像进行预处理。

预处理通常分为指纹图像分割、增强、二值化等步骤，每个步骤对预处理的后续步骤都有重要的意义。下面我们将分别介绍这三个步骤。

4.3.1　指纹图像分割

指纹图像分割就是在采集到的指纹图像中找到包含所有指纹有效信息的区域，并去除有效区域外的其它区域的过程。有效区域也称指纹图像的前景区域，除前景区域外的其它区域称为背景区域，图 4-5 中闭合曲线内部的区域就是指纹的前景区域，闭合曲线外部的区域就是指纹的背景区域。

自动指纹识别系统中进行指纹匹配时所需要的是由清晰的脊线谷线所组成的指纹区域的指纹图像。但是在指纹图像的采集过程中，真实的指纹图像通常都含有大量的噪声，这些噪声会使指纹特征提取产生错误，进而影响指纹的匹配精度。指纹图像分割可以去除非指纹区域的影响因素，提取到真实的指纹纹理区域信息，从而提高特征提取的正确率，提高自动指纹识别系统的整体性能。

自动指纹识别系统中指纹图像分割技术已经做得比较成熟，常用的指纹图像的分割算法有：(1)基于边缘检测的方法；(2)基于多特征分类器的指纹分割；(3)基于人工神经网

(a)　　(b)

图 4-5　指纹图像分割图:闭合曲线内部分是分割后的前景区域,其它部分是背景区域

络 ANN 的方法;(4)基于马尔科夫模型的方法等。本书将在第 7 章对指纹图像的分割技术进行详细的介绍。

4.3.2　指纹图像增强

指纹图像增强就是通过一定的增强算法对分割后的存在噪声的指纹图像进行处理,使得指纹的纹理变得清晰,脊线和谷线之间的对比度得到增强,同时保留真实的特征信息,尽量去除伪特征信息的过程,如图 4-6 所示。

(a)原指纹图像　　(b)增强后的指纹图像

图 4-6　指纹图像增强图

在自动指纹识别系统的指纹采集过程中,难以直接获得清晰的、没有噪声的指纹图像。指纹传感器、被采集对象的手指的自身条件和外界环境都会影响指纹图像采集的结果。采集到的指纹图像中出现很多噪声,脊线中也存在不同程度的模糊、变形、粘连和断裂。如果直接使用这种质量不好的图像进行指纹特征提取和指纹匹配,那么指纹特征提取的准确性以及指纹匹配的结果都会受到很大的影响。因此,为了提高自动指纹识别系

统的识别精度，我们需要对指纹图像进行增强处理。指纹图像的增强处理也是指纹识别系统中非常关键的步骤。

指纹图像增强的算法有很多，常用的指纹增强算法有：(1)基于 Gabor 滤波的指纹图像增强算法；(2)指纹图像的自适应滤波增强算法；(3)基于像素的指纹图像增强算法；(4)基于 STFT 的指纹图像增强算法等。本书将在第 8 章对指纹图像的增强做详细的介绍。

4.3.3　指纹图像二值化

指纹图像二值化就是将增强后的指纹灰度图像转换为只有 0、255 两个值的二值图像的过程。二值化可以将脊线和谷线分别变为黑、白像素，从而使指纹特征信息更为清晰，如图 4-7 所示。

(a) 增强后的指纹图像　　(b) 二值化后的指纹图像

图 4-7　指纹图像二值化图

指纹图像二值化处理是自动指纹识别系统的预处理中一个非常重要的步骤。在指纹图像的识别过程中，指纹图像是由大量的 256 级的灰度像素组成的，而脊线的走向是指纹图像中重要的信息。在识别过程中，我们不需要知道图像中每个像素的具体的灰度值，只需要知道每个点的值是 0 或者非 0。因此我们就可以把指纹图像中所有的像素点二值化，把脊线上的像素点的灰度转变为 0，不在脊线上的点的灰度转变为 255。

对指纹图像进行二值化处理，既对指纹图像信息进行了压缩、减少了数据总量、节约了存储空间、便于计算机存储和处理，同时又能保留指纹图像中最重要的信息。除此之外，指纹图像二值化处理还可以去除指纹脊线的错误连接，为指纹特征的提取和匹配做好准备。

二值化的方法很多，关键在于阈值的选取。常用的二值化方法有：固定阈值法、动态阈值法。我们可以根据图像的特点选择合适的二值化方法对图像进行二值化处理。本书将在第 8 章对指纹图像的二值化处理进行详细介绍。

4.4　指纹特征提取

指纹特征提取就是从一幅含有大量信息的指纹图像中，获得一些有区别能力的、稳定的并且能表现出不同指纹的差异的特征点的过程，如图 4-8 所示。

(a)　　(b)

图 4-8　指纹特征提取图:(a)、(b)中红色标记的点为细节点

一幅指纹图像中含有大量的数据,将所有的数据都用于指纹图像的匹配是不现实的。因为数据量太大,会大大增加匹配所用的时间。因此从指纹图像中获取到具有代表性的指纹特征用于指纹匹配是非常必要的。

指纹存在两种特征,即全局特征和局部特征。全局特征用于指纹的分类,它指的是指纹中脊线的总体走向。根据全局特征可以将指纹分成 5 种类型:左旋型、右旋型、螺旋型、拱型和尖拱型。局部特征是指指纹图像中的细节特征,例如指纹脊线的突然停止所形成的终结点,指纹脊线的突然分叉所形成的分叉点,孤立的一小段脊线所形成的小岛,以及连接两条脊线的桥等。

指纹图像的全局特征通常用于指纹图像的分类与检索,而指纹图像的局部特征常用于匹配。目前最常用的指纹匹配方法是美国联邦调查局(FBI)采用的基于指纹特征点的匹配方法,它所用于匹配的指纹特征就是指纹的局部特征。

指纹特征点的提取有两种方法,一种是基于细化图像的,如利用 8 邻域模板法提取特征点;另一种是基于灰度图像的,如利用链码(ChainCode)提取指纹特征点。本书将在第 9 章对利用链码提取指纹特征点的方法进行详细的介绍。

4.5　指纹匹配

指纹匹配就是利用从两幅指纹图像中提取到的特征数据进行比较,判断两个指纹图像是否来自于同一手指的过程,如图 4-9 所示。如果匹配的分数大于我们所设定的阈值,那么认为这两个指纹是匹配的,如果小于设定的阈值,则认为是不匹配的。指纹匹配是自动指纹识别系统中最关键的步骤,指纹匹配算法的好坏直接影响到自动指纹识别的结果。

指纹匹配过程中,通常将提取到的多个细节点的相对位置、方向等参数信息形成一个数据集合,从而将指纹的匹配问题转化为特征点集合的相似性问题。在实际的应用过程中,指纹图像的采集会出现指纹位置偏移、指纹图像非线性形变,以及指纹图像残缺等问题。这些问题导致了采集到的一枚手指的两个指纹所包含的信息不完全相同,指纹匹配问题在这里就转化为一个模糊匹配的过程,根据模糊匹配分数利用阈值法判定匹配结果。

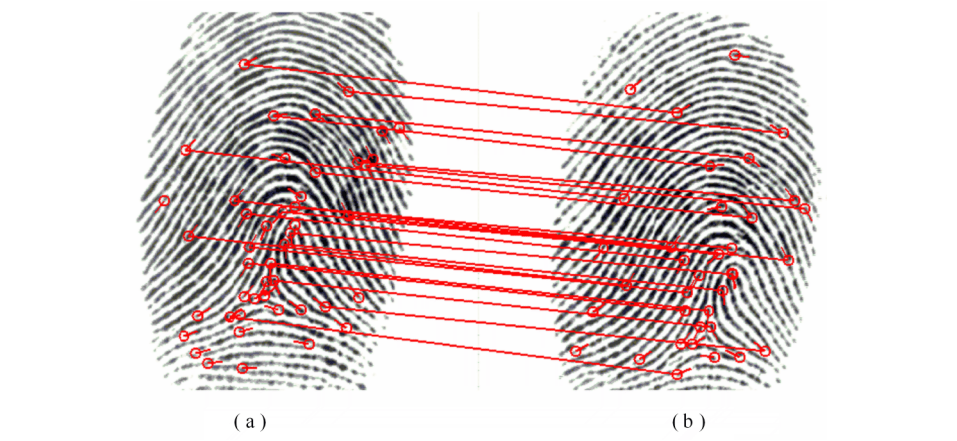


图 4-9　指纹特征匹配图:(a)、(b)分别为同一手指的不同指纹图像,
蓝色和红色的圈分别代表细节点,绿色的线连接相匹配的点

目前指纹的匹配方法有很多,有细节点模式匹配法,图论匹配法,基于神经网络的匹配法、基于细节点特征和纹理特征的匹配法等。本书将在第 9 章对基于方向描述子(Tico 算子)的指纹图像匹配法进行详细介绍。

4.6　生物特征加密系统

生物特征加密系统就是利用提取到的生物特征和密钥进行绑定,实现对用户重要信息进行加密保护的系统。生物特征的种类有很多,如指纹、掌纹、人脸、虹膜、视网膜、静脉、语音、步态以及签名等。指纹识别作为最成熟、便捷、精确的生物特征识别技术,首先被应用到生物特征加密技术中。

生物特征加密技术是一个把密钥和生物特征安全地绑定到一起的过程,使得密钥和生物特征本身都不能从系统存储的模版中获取到,当且仅当活体生物特征提取交给系统并且与存储在系统中的模板相匹配时,密钥才会重新生成。

基于指纹识别的生物特征加密系统首先要输入注册的指纹并提取特征数据,然后将指纹的特征数据与密钥绑定到一起。只有再次输入的验证指纹的特征数据能与注册的指纹特征数据相匹配,才能解绑出密钥,解绑出的密钥将用于其它信息的加密与解密。

本书将在第 10 章对模糊保险箱(Fuzzy Vault)算法进行详细介绍。该算法很好地将生物特征的模糊性与密码技术的精确性融合在了一起,对信息的保护有着很好的效果。

4.7　本章小结

本章介绍了自动指纹识别系统与加密系统的基本框架和功能。从指纹图像的采集、预处理、特征提取、指纹匹配和指纹加密几个方面展开讨论,并介绍了每个步骤的基本概念和常用方法。

随着自动指纹识别系统与加密系统在我们的日常生活中的应用越来越广泛,人们对

自动指纹识别系统与加密系统的识别速度、精度和安全性的要求也进一步提高。如何进一步提高自动指纹识别系统与加密系统的速度、精度和安全性也成为近年来该领域的研究热点。

习题与思考题

1. 自动指纹识别系统的组成部分有哪些，分别有什么作用？
2. 你认为自动指纹识别系统中最重要的部分是哪个？原因是什么？
3. 在你的日常生活中，哪些地方用到了自动指纹识别系统？你认为自动指纹识别系统能否在日常生活中得到广泛的应用？
4. 与其它识别方法（如身份证、ID 卡等）相比，自动指纹识别系统有什么优势，又有什么劣势？
5. 谈谈你对生物特征加密的理解。
6. 生物特征加密的应用场景有哪些，你认为这种方法的安全性能否满足实际应用？
7. 在日常生活中，你会不会使用生物特征加密的方法来保护自己的信息，并阐述原因。

第 5 章　指纹识别算法性能评价

指纹识别算法的性能直接影响到自动指纹识别系统的应用。目前，对指纹识别算法的评价主要基于国际上流行的标准指纹数据库上运行算法所获取的性能指标。本章首先介绍当前国际上使用最为广泛的几种标准指纹数据库以及其它的一些指纹数据库，然后结合标准数据库对评价指纹识别算法性能的重要指标进行说明，最后我们给出了目前在手机和移动端中十分流行的中等面积指纹识别算法的性能评价方法。

本章内容：5.1 节介绍了几种常用的指纹数据库，5.2 节介绍常规指纹识别算法的评价方法，5.3 节介绍应用级指纹识别算法的评价方法，5.4 节总结本章的内容。

5.1　指纹识别数据库

指纹识别数据库是按照一定的规则采集指纹图像而形成的图像数据集合。指纹数据库可以用于测试指纹识别算法性能，也可以用于对指纹分类检索等问题的研究。目前国际上主流的指纹数据库包括 NIST 指纹数据库、FVC 指纹数据库等，下面我们将详细介绍各数据库的内容和特点。

5.1.1　NIST 指纹数据库

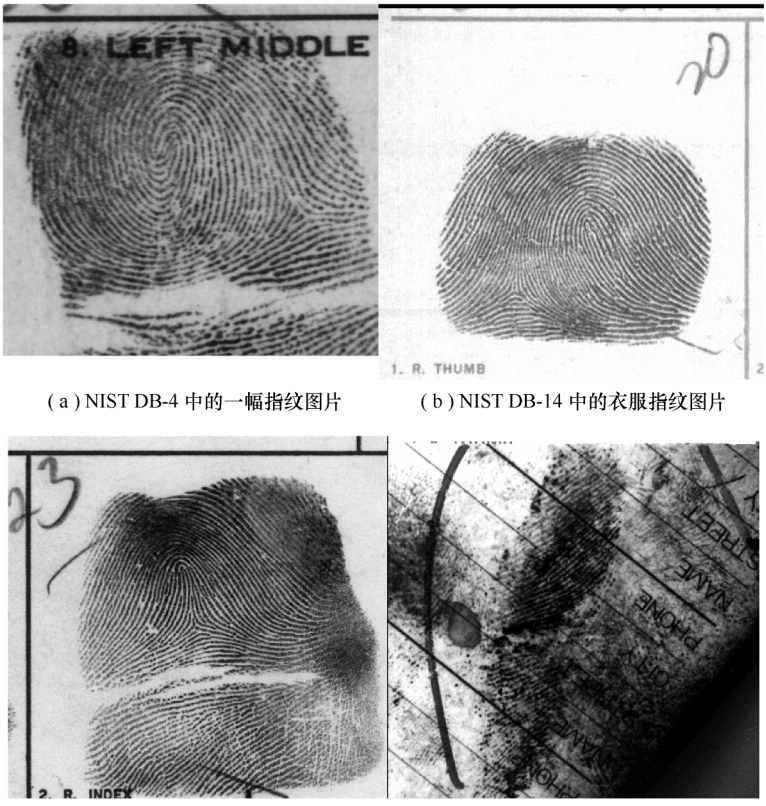
NIST(National Institute of Standards and Technology)是美国国家标准局的缩写，该局直属于美国商务部，从事物理、生物和工程方面的基础和应用研究，并在众多领域提供了国际化的标准和标准参考数据，在国际上享有很高的声誉。NIST DB-4、NIST DB-9、NIST DB-10、NIST DB-14、NIST DB-24、NIST DB-27 是美国国家标准局所颁布的标准指纹库。NIST 指纹数据库对自动指纹识别系统的发展和指纹分类的研究起了重要的作用，它是指纹理论研究中评价优秀算法性能的常用数据库。

NIST 的每个数据库都有其不同的特点。NIST DB-4 和 NIST DB-9 是在 1992 年建立的，NIST DB-10 和 NIST DB-14 是在 1993 年建立的，这 4 个数据库的建立时间较早，主要的采集方式是扫描用油墨按压在指纹卡上的指纹，图像如图 5-1(a)、(b)所示，这种方式扫描的图像与现在实时指纹采集的指纹图像有很大的差异。

NIST DB-24 的指纹图像的存储形式是图片序列形式，每个指纹表现为 10 秒钟(300 帧)具有弹性形变的图像序列以及 10 秒钟各个角度的图像序列。静态的图片也可以从图片序列中提取出来用于指纹识别算法评估。

NIST DB-27 的指纹图像主要用于潜指纹识别，潜指纹是在某些特殊场合采集到的不完整的指纹。NIST DB-27 中包括了一个全指纹集和一个潜指纹集，如图 5-1(c)、(d)所示，它们是一一对应的。潜指纹的识别在刑侦领域起着关键性的作用，因为案发现场留下来的指纹大部分是不完整的。值得一提的是，NIST DB-27 库中每个指纹除了 10 副图

像外，还额外给出了 4 个专家标出的细节点集，细节点集对指纹识别算法的评价有着很高的参考价值。



(a) NIST DB-4 中的一幅指纹图片　(b) NIST DB-14 中的衣服指纹图片

(c) NIST DB-24 中的一幅全指纹图像　(d) NIST DB-24 中与 (c) 对应的浅指纹图像

图 5-1　NIST 数据库指纹图片

NIST 标准指纹数据库的每一个库在采集形式、图片数量、图片存储格式和图片大小等方面均不相同。表 5-1 对 NIST 部分指纹库的参数进行了详细的介绍。

表 5-1　NIST 部分指纹数据库参数

数据库	NIST-4	NIST-9	NIST-14	NIST-24	NIST-27
图像数量	2000 对	270 对	27000 对	100 个	2580 个
格式	JPEG	JPEG	WSQ	MPEG-2	ANSI/NIST-ITL 1-2000
图像大小	512×512 像素	832×768 像素	832×768 像素	720×480 像素	800×768 像素
应用	自动指纹分类	自动指纹分类	自动指纹分类	自动指纹认证	自动指纹认证

NIST 指纹数据库为自动指纹识别系统和指纹分类等研究的发展做出了巨大贡献，但随着指纹识别技术的发展，对于实时扫描指纹识别的应用越来越多，而 NIST 数据库中的大部分图片不是采集的实时指纹，因此不适用于实时指纹识别算法的性能评价。FVC 数据库则从一定程度上弥补了 NIST 数据库的不足，下面我们将对 FVC 数据库进行介绍。

5.1.2　FVC 数据库

FVC(Fingerprint Verification Competition)是国际模式识别协会 IAPR(International Association of Pattern Recognition)举办的指纹算法竞赛,该竞赛的宗旨是为所有对指纹识别算法感兴趣的研究人员提供一个标准指纹数据库,并追踪当前算法性能的发展轨迹。目前为止,FVC 已经成功举办了 4 届(2000 年、2002 年、2004 年、2006 年),此后,FVC 在其官网提供了 FVC－ongoing 在线测评服务,供广大研究考测试算法的性能并比较优劣。4 届竞赛中使用的分别是 FVC2000、FVC2002、FVC2004 和 FVC2006 指纹认证数据库,它们是用于算法评测的最新标准数据库。在每个 FVC 数据库中分别包含了 4 个不同的子指纹数据库:DB1、DB2、DB3 和 DB4,这 4 个子数据库在识别的难度上略有不同,造成识别难度不同的原因主要有人口的差异、志愿者采集过程中的配合程度,以及采集仪种类不同等。下面分别对每个数据库进行介绍。

FVC2000 数据库中包含了 110 个手指,每个手指 8 幅,共 880 幅指纹图像。每个子数据库的具体参数如表 5-2 所示,数据库指纹样图如图 5-2 所示。

表 5-2　FVC2000 数据库参数

子数据库	DB1	DB2	DB3	DB4
采集仪	KeyTronic 公司 Secrue Desktop Scanner 光学采集仪	ST Microelectronics 公司 TouchChip CMOS 采集仪	Identicator Technology 公司 DF-90 光学采集仪	意大利博洛尼亚大学的指纹合成软件 SFinGe
图像大小	300×300	256×364	448×478	240×320
分辨率	500 dpi	500 dpi	500 dpi	约 500 dpi

(a) DB1 中的指纹图片　(b) DB2 中的指纹图片　(c) DB3 中的指纹图　(d) DB4 中的指纹图片

图 5-2　FVC2000 数据库中的图片

FVC2002 数据库中包含了 110 个手指,每个手指 8 幅,共 880 幅指纹图像。每个子数据库的具体参数如表 5-3 所示,数据库指纹样图如图 5-3 所示。

表 5-3　FVC2002 数据库参数

子数据库	DB1	DB2	DB3	DB4
采集仪	Identix 公司 TouchView2 光学采集仪	Boimetrika 公司 FX2000 光学采集仪	Precise Biometric 公司 100SC 电容式采集仪	意大利博洛尼亚大学的指纹合成软件 SFinGe V2.51
图像大小	388×374	296×560	300×300	288×384
分辨率	500 dpi	500 dpi	500 dpi	约 500 dpi

(a) DB1 中的指纹图片　(b) DB2 中的指纹图片　(c) DB3 中的指纹图片　(d) DB4 中的指纹图片

图 5-3　FVC 2002 数据库中的图片

FVC 2004 数据库中包含了 110 个手指，每个手指 8 幅，共 880 幅指纹图像。每个子数据库的具体参数如表 5-4 所示，数据库指纹样图如图 5-4 所示。

表 5-4　FVC2004 数据库

子数据库	DB1	DB2	DB3	DB4
采集仪	CrossMatch 公司的 V300 光学采集仪	Digital Persona 公司的 U. are. U 4000 光学采集仪	Atmel 公司 FingerChip FCD4B14CB 热敏采集仪	意大利博洛尼亚大学的指纹合成软件 SFinGe V3. 0
图像大小	640×480	328×364	300×480	288×384
分辨率	500 dpi	500 dpi	512 dpi	约 500 dpi

(a) DB1 中的指纹图片　(b) DB2 中的指纹图片　(c) DB3 中的指纹图片　(d) DB4 中的指纹图片

图 5-4　FVC2004 数据库中的图片

FVC2006 数据库中包含了 150 个手指，每个手指 12 幅，共 1800 幅指纹图像。每个子数据库的具体参数如表 5-5 所示，数据库指纹样图如图 5-5 所示。

表 5-5　FVC2006 数据库参数

子数据库	DB1	DB2	DB3	DB4
采集仪	Authentec 公司 AES 4000 光学采集仪	Biometrika 公司 FX3000 光学采集仪	Atmel 公司 FingerChip 热敏采集仪	意大利博洛尼亚大学的指纹合成软件 SFinGe V3. 0
图像大小	96×96	400×560	400×500	288×384
分辨率	250 dpi	569 dpi	500 dpi	约 500 dpi


(a) DB1 中的指纹图片


(b) DB2 中的指纹图片


(c) DB3 中的指纹图片


(d) DB4 中的指纹图片

图 5-5　FVC2006 数据库中的图片

FVC 数据库相对于 NIST 数据库而言，其图像更适合实时指纹识别算法的测试和评价。FVC 指纹数据库基本满足了对大多数指纹识别算法的性能进行评估的要求，读者如需测试自己的算法，可酌情选择 FVC 的不同数据库。

5.1.3　其它数据库

除了 NIST 和 FVC 数据库外，国际上还有一些指纹数据库可以用于指纹识别算法性能检测。下面推荐的一些数据库均包含了指纹在内多种生物特征，可以用于多模态生物特征识别算法的评价和测试。

1. MCYT 双模态生物特征数据库

由 Ortega-Garcia 等人建立于 2003 年，该数据库包含了来自了 330 个志愿者的指纹和签名数据。

2. BIOMET 多模态生物特征数据库

由 Garcia-Salicetti 等人建立于 2003 年，该数据库包含了 91 个志愿者的语音、人脸、手型、指纹和签名数据。

3. BioSec 多模态生物特征数据库

由 Fierrez-Aguilar 等人建立于 2007 年，包含了 250 个志愿者的人脸、语音、指纹以及虹膜数据。值得一提的是，FVC2006 的 DB1、DB2 和 DB3 三个子数据库是来源于这个数据库的。

4. BioSecure 多模态生物特征数据库

由 BioSecure 建立于 2008 年，该数据库由三个子数据库组成，DB1 包含了 1000 个来源于网络无监管志愿者的人脸和语音数据；DB2 包含了 700 个志愿者在标准办公室环境下采集到的人脸、声音、签名、指纹、手型和虹膜数据；DB3 包含了 700 个志愿者使用手持设备在室内受控或室外不受控两种环境下采集的人脸、声音、签名和指纹数据。

我国在指纹数据库方面也做出了贡献，中国科学院自动化所联合组织举办的 BVC 2004(Biometrics Verification Competition 2004)和 BAC 2005(Biometrics Authentication Competition 2005)两届生物特征识别竞赛也提供了两个相应的数据库。BVC 组织方提

供了 5 个不同的指纹子数据库，DB1、DB2、DB3、DB4 和 DB5。每个数据库有 220 个手指的指纹，每个手指采集了 10 幅图像，总计 2200 幅图像，表 5-6 给出了 BVC 数据库的信息。

BAC 2005 的组织方提供了 4 个不同的指纹数据库，DB1、DB2、DB3 和 DB4，用于参赛算法的测试和训练，表 5-7 给出了 BAC 2005 各数据库的信息。

表 5-6　BVC 数据库信息

数据库	DB1	DB2	DB3	DB4	DB5
采集仪类型	光学采集仪	CMOS 采集仪	热敏采集仪	指纹生成器	卡片指纹
图像大小	412×362	256×300	300×480	400×460	440×352
分辨率	500 dpi	500 dpi	500 dpi	500 dpi	500 dpi

表 5-7　BAC 2005 数据库信息

数据库	DB1	DB2	DB3	DB4
采集仪类型	光学采集仪	CMOS 采集仪	刮擦采集仪	指纹生成器
图像大小	640×480	128×128	256×400	380×460
分辨率	500dpi	250dpi	500dpi	500dpi

除了 BVC 和 BAC 数据库外，中科院自动化所还建立了多采集仪指纹数据库，包含了一个手指在不同采集仪上采集的指纹数据，方便进行多个采集仪交叉匹配的研究。这个数据库包含了 9 个子数据库，是由 90 个志愿者的 8 个手指在 9 种采集仪上每个采集 12 幅图像构成的，总计 8640 枚指纹图像。多采集仪指纹数据库的信息如表 5-8 所示。

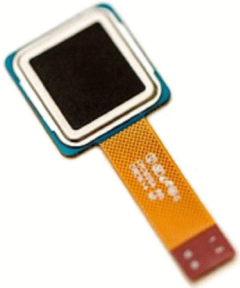
表 5-8　交叉指纹数据库信息

数据库	DB1	DB2	DB3	DB4	DB5	DB6	DB7	DB8	DB9
采集仪	光学	光学	光学	刮擦	刮擦	刮擦	电容电感	电容电感	电容电感
图像尺寸	400×560	640×480	500×550	不固定	124×400	288×384	144×144	152×200	208×288
分辨率	569dpi	500dpi	700dpi	500dpi	250dpi	500dpi	500dpi	363dpi	500dpi

西安电子科技大学庞辽军教授领导的生物特征加密研究组在 2015 年建立了 XDFinger 指纹数据库。该数据库包含了来自 150 名志愿者的 1500 幅指纹图像，采集规则是每个志愿者任选除小拇指外的 8 个手指中的 1 个作为采集手指，采集该手指的 10 幅图像。目前，XDFinger 数据库还在持续建设中，随着越来越多的志愿者加入，该数据库的容量也将不断增加。

XDFinger 数据库的构建满足了当今手机市场中主流的中等面积(190×190 左右)指纹识别算法的测试需求，该数据库使用的采集仪是瑞典指纹卡公司(Fingerprint Cards，FPC)的 FPC1020 触摸式采集仪。该款采集仪特点是采集指纹面积较小，图像有效尺寸为 192×192。目前市场上很多手机采用了 FPC1020 采集仪，如华为的 Mate7、纽曼的 CM810。而其同系列的 FPC1021、FPC1024 及 FPC1025 等采集仪则广泛用于华为、中兴、魅族、酷派等手机终端上。图 5-6(a)是 FPC1020 指纹采集仪，图 5-6(b)则是使用该采

集仪获得的指纹图片。



(a) 采集仪

(b) 图像

图 5-6　FPC 1020 指纹采集仪和它采集的图像

指纹识别算法的优劣是在指定的数据库上进行评价的，下一节我们介绍常规指纹识别算法的性能评价。

5.2　常规指纹识别算法性能评价

指纹识别算法的性能是评价一个自动指纹识别系统性能的重要指标。因此，在评价指纹识别算法时，通常需要在标准的数据库上使用标准的评价方法，只有如此，方能证明算法的科学性和实用性。比如，2000 年，国际模式识别组织提出了 FVC2000 算法评估方案，这个方案后来成为一种公认的指纹识别算法性能评价标准，它详细的定义了拒识率(FRR)、误识率(FAR)、等错误率(EER)、匹配时间等一系列指标和计算方法。需要注意的是，多数的评价指标(如拒识率和误识率等)同样适用于其它生物特征识别算法的性能评价，评价方法也十分相似，本书以指纹为例进行介绍。

5.2.1　系统错误的产生

在理想的指纹识别系统中，输入的样本会得到一个正确的决策，如是否匹配，是否通过等。但实际上，一个指纹识别系统是一个模式识别系统，它会不可避免地做出一些错误的判断，正是如此，现实中指纹识别算法的准确率不会达到 100%。下文我们将介绍指纹识别系统会带来的系统错误，并讨论错误的类型。产生系统错误的类型和原因主要有以下三种：

1. 信息限制

信息限制是指系统可以从生物特征中获取的信息量大小会受到限制的，这种限制通常分为两种：一种是生物特征本身存在信息容量的限制，比如人手掌的几何信息量要少于指纹的信息量；另一种是由于采集不当而未获得足够的信息，比如在两次采集指纹的过程中分别采集到了手指左右两边不同的指纹信息。

2. 表达限制

理想状态下表达一个生物特征时我们希望可以最大程度的保留其不变性和可辨识性,但在实际情况中,我们可能无法获得丰富的特征信息,并导致正确信息丢失,错误信息保留。

3. 不变性限制

对于同一个指纹,我们通常希望每次采集到的特征能够保持不变,而在实际情况中,同一手指的指纹在多次采集的时候往往会发生变化。

由上述三种限制产生的系统错误类型有很多种,如指纹获取模块中的探测失败(failure to detect,FTD)错误;捕获失败(failure to capture,FTA)错误;特征提取模块中的处理失败(failure to process,FTP);模板创建过程中的注册失败(failure to enroll,FTE)错误。在匹配阶段,用以描述匹配结果的是误识率(false acceptance rate,FAR)和拒识率(false rejection rate,FRR)两个指标,误识率和拒识率最为直观的反映了一个指纹识别算法的性能,下一节我们将详细介绍拒识率和误识率这两个指标的概念。

5.2.2 误识率和拒识率

在介绍误识率和拒识率之前,我们首先需要了解指纹识别算法中匹配分数的概念,匹配分数是算法中自行设计的,用于判断两个指纹相似程度的量化标准。通常认为匹配分数越大,两个指纹图像来自于同一个手指的概率越高,算法的设计者会设定一个匹配分数的阈值,当两幅指纹图像的匹配分数高于这个阈值时,认为两个指纹是匹配的,反之认为是不匹配的。

误识率是指在标准指纹数据库上测试指纹识别算法时,不同指纹的匹配分数大于给定阈值,从而被认为是相同指纹的比例,简单地说就是“把不应该匹配的指纹当成匹配的指纹”的比例,它是用来评估指纹识别算法性能的最重要参数。

拒识率是指在标准指纹数据库上测试指纹识别算法时,相同指纹的匹配分数低于给定阈值,从而被认为是不同指纹的比例,简单地说就是 “把应该相互匹配成功的指纹当成不能匹配的指纹”的比例。

下面使用一个例子来具体介绍拒识率和误识率的计算方法。假设使用 FVC2000 DB1 指纹数据库测试指纹识别算法性能时,计算误识率的方法如下:指纹库中有 110 个不同 ID 的手指,每个手指注册有 8 枚指纹,则共有 880 枚指纹。假定 F1_1,F1_2,…,F1_8 表示手指 1 的 8 幅指纹图片,把库中的每个指纹,与除自己之外的其它所有指纹进行匹配,匹配的总次数,即 880×(880−1)=773520 次。理论情况下,来自同一个指纹的图像都成功匹配,次数为次,匹配失败次数应为 773520−6160=767360 次。假定由于指纹识别算法性能的原因,把本应该匹配失败的判为匹配成功,若假定这种错误次数为 1000 次。则误识率(FAR)为$\frac{1000}{767360}\times 100\%=0.134\%$。匹配失败次数是因匹配分数设计的条件严格程度而变化的。当匹配分数的阈值设置得越高时,FAR 会降低。

计算拒识率的方法是把指纹库中的同一个手指的 8 枚指纹两两比较，共有 7×8＝56 种匹配方式。把所有 110 个手指在其内部均作 56 种匹配，共 56×110＝6160 次匹配。理论情况下，6160 次匹配均能正确匹配，匹配的成功率为 100%。实际上因为同一手指的 8 枚指纹图像不可能完全一样，具体表现为匹配分数不可能都高于阈值，假定高于阈值的次数为 6000 次，则剩余的 160 次匹配分数均均低于阈值，则拒识率就是 160/6160×100%＝2.6%。

计算出误识率和拒识率后，下一节我们将介绍 ROC 曲线和等错误率，这两种方式更为直观的表现了指纹识别算法的性能和不同性能的适用情景。

5.2.3　ROC 曲线和等错误率

ROC 曲线（Receiver Operator characteristic Curve）是一种已经被广泛接受的指纹识别系统匹配算法测试指标，它是匹配分数阈值、误识率以及拒识率之间的一种关系。它反映了指纹识别算法在不同阈值上，拒识率和误识率的平衡关系，图 5-7 给出了 ROC 曲线，其中横坐标是拒识率，纵坐标是误识率，等错误率（Equal－Error Rate，EER）是拒识率和误识率的一个平衡点，等错误率能够取到的值越低，表示指纹识别算法的性能越好。

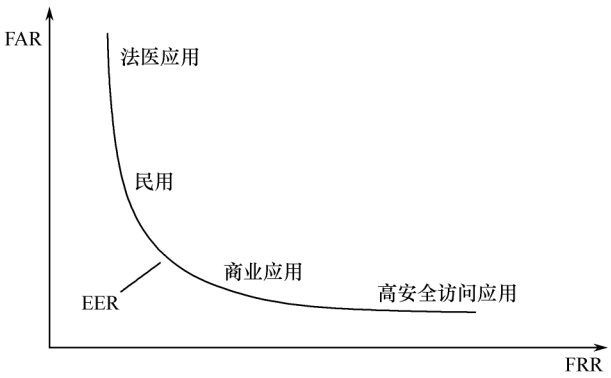


图 5-7　ROC 曲线

拒识率和误识率不可能同时达到最低，因此，不同的指纹识别算法会针对不同的使用环境，如在司法和刑侦应用中，可以接受较高的误识率，即允许锁定大范围的可疑指纹并逐一进行排查，但不能接受可疑指纹的遗漏；在需要较高安全性应用的场合，如在银行系统中，为了保证用户的经济安全，可以接受较高的拒识率，即合法用户被拒绝时可以通过二次录入再次认证，但不允许出现非法用户能够认证通过的情景。

5.3　应用级指纹识别算法性能评价

5.2 节我们对常规指纹识别算法性能的评价做了详细的介绍，本节我们将以当今手机和移动设备上流行的中等面积指纹为例，介绍应用级指纹识别算法性能的评价。

应用级指纹识别算法的评价标准与常规指纹的评价标准略有不同，在实际应用中，指纹识别算法应该更关注能否获得良好的用户体验，即算法是否能够准确快速的识别合法用户的指纹且拒绝不合法用户的指纹。因此，应用级指纹识别算法在模板构建和实时匹配过程中的算法设计都与常规指纹算法不同。

西安电子科技大学生物特征加密团队对中等面积指纹的识别算法进行了长足的研究，并建立了中等面积指纹数据库 XDFinger。下文给出在中等面积指纹识别算法设计中模板构建和匹配两个阶段的设计思路。

1. 模板构建

中等面积指纹的特点在于它的采集面积在 190×190 左右，因此所包含的指纹信息要比常规指纹少很多，图 5-8 给出了源于同一个手指的指纹图像的对比，其中图(a)为中等面积指纹，图(b)为常规指纹，其中方框部分面积与图(a)重合。

(a) 中等面积指纹　　(b) 常规指纹

图 5-8　来源于同一个指纹的图像对比

可以看出中等面积指纹包含的指纹面积要比常规指纹少很多，基本相当于方框中的面积，因此获得的用于匹配的特征也就相对较少。在模板构建阶段，中等面积指纹通常获取同一个手指的不同区域 5～10 幅指纹图像，作为一个混合模板，并用于后续的匹配。

2. 匹配

由于指纹模板构建的特殊性，中等面积指纹的匹配方案也与常规指纹有所不同。在我们的 XDFinger 数据库中，有来自于 150 名志愿者的 1500 幅指纹图像，每个手指 10 幅。在计算误识率时，用每一个手指的一个模板与其它手指的 10 个模板进行匹配，找出最大的匹配分数，作为两个手指间的匹配分数，总计进行 1500×(1500－1)＝2248500 次匹配，若在匹配期间，有 2000 次是超过匹配分数阈值，即错误匹配的，此时误识率为 2000÷2248500×100%＝0.089%。在计算拒识率时，需要用每个手指的一个模板与本手指的其它 9 个模板进行匹配，找到分数最高的作为两个指纹的匹配分数，总计进行 1500×9＝13500 次匹配，若匹配期间有 10 次匹配的匹配分数低于阈值，则拒识率为 10÷13500×100%＝0.074%。

得到了拒识率和误识率以后，可以根据上一节计算 ROC 和 EER 的方法进行计算，图 5-9 是某次真实算法测试得到的 ROC 曲线，图 5-10 用另一种直观方式表现了 EER 的取值。

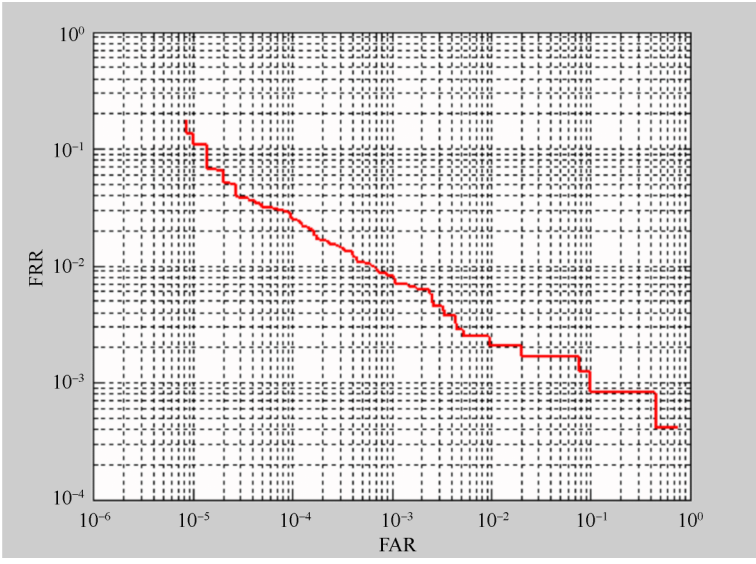


图 5-9　真实算法测试的 ROC

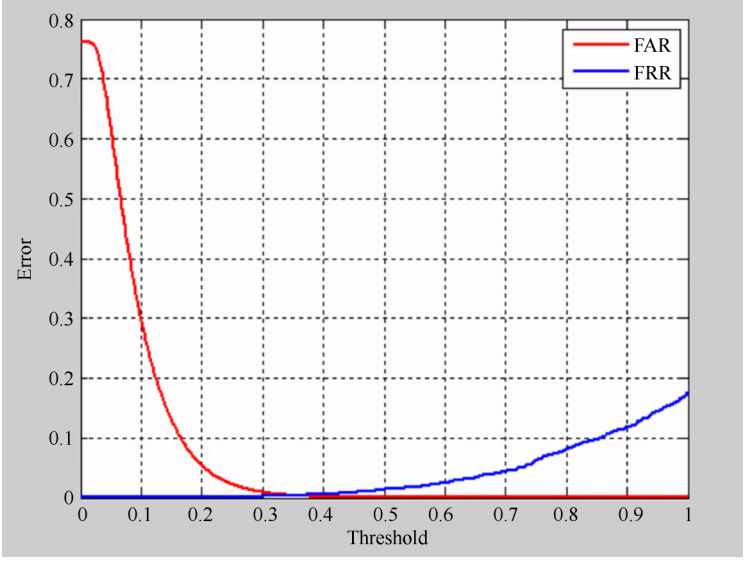


图 5-10　EER 曲线，蓝线表示误识率，红线表示拒识率，两个曲线的交点为 EER

5.4　本章小结

本章主要介绍了指纹识别算法的性能评价方法。首先介绍了国际国内用于测试指纹识别算法性能的标准数据库和它们的数据特点，然后结合 FVC 数据库介绍了常规指纹识

别算法的评价指标和评价指标的计算方法，最后，介绍了当下应用在在手机和移动端的中等面积指纹识别算法的评价方法，并结合 XDFinger 数据库介绍了算法的评价指标。

习题与思考题

1. 你认为 NIST 数据库还适用于今后的指纹识别算法性能评价吗？
2. FVC 数据库的特点是什么，它和 NIST 数据库分别适用于哪类指纹识别算法测试？
3. 你能否想到其它影响到指纹识别算法性能的原因？
4. 拒识率和误识率能否同时达到最低？
5. 从应用的层次来讲，误识率和拒识率哪一个是你比较关心的？

第 6 章　指纹图像的采集

指纹图像的采集就是获取数字指纹图像的过程，也是自动指纹识别系统的第一步。采集到的指纹图像的质量好坏将直接影响对指纹图像进行预处理、特征提取和匹配等后续处理步骤，最终对指纹识别系统的识别结果产生重大的影响。

因为指纹表面积较小，且存在磨损，所以获取优质指纹图像较困难。指纹传感器是获取指纹图像的专用器件，因此在自动指纹识别系统中指纹传感器起着关键作用。

本章将从以下几个方面来介绍指纹图像的采集：6.1 节介绍指纹采集的发展，6.2 节介绍指纹传感器的分类，6.3 节介绍指纹传感器的原理，6.4 节介绍指纹传感器的性能比较，6.5 节本章内容总结。

6.1　指纹采集的发展

早期的指纹图像是通过油墨按印等物理方式采集的，如图 6-1 所示，NIST4、NIST9 等标准指纹数据库就属于这一类。油墨或纸张质量有问题、按压位置、按压压力不均、变形、方向差异、手指损伤等都会导致采集的指纹图像质量不理想，进而影响指纹识别的结果。

图 6-1　油墨采集指纹图像

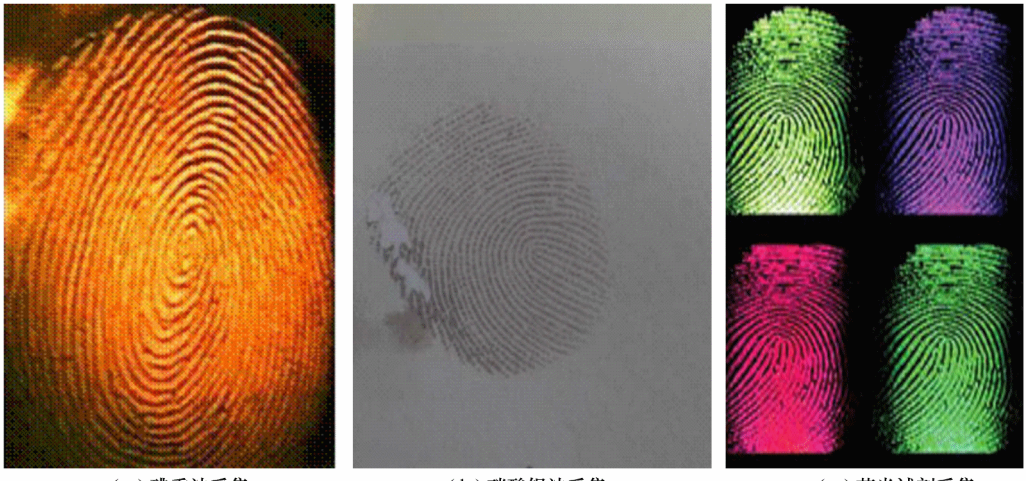
现场指纹图像可以通过物理方法和化学方法来获取。

物理方法适用于指纹遗留在金属、塑胶、玻璃、瓷砖等非吸水性物品的表面。常见的物理方法有粉末法和磁粉法。粉末法是选择颜色对比大的粉末，撒在指纹遗留地，这样就能提取完整的指纹；磁粉法是以微细的铁粉颗粒，用磁铁作为刷子，来回刷扫，就可以显示出指纹图像，如图 6-2 所示。

化学方法适用于纸张、卡片、皮革、木头等吸水性物品的表面。常见的化学方法包括碘熏法、宁海得林(Ninhydrin)法、硝酸银法和荧光试剂法。碘熏法是利用碘晶体加温产生蒸汽，它与指纹残留物的油脂产生反应后便会出现黄棕色的指纹并且必须立即拍照或

图 6-2　使用磁性粉末法提取的指纹图像

者用化学方法固定，如图 6-3(a)所示；宁海得林法是将试剂喷在检体上，与身体分泌物的氨基酸产生反应后会呈现出紫色的指纹；硝酸银法是利用硝酸银溶液与潜伏指纹中的氨化钠产生反应后，在阳光下会产生黑色的指纹，如图 6-3(b)所示；荧光试剂法是利用荧光氨与邻苯二醛快速与指纹残留物的蛋白质或氨基酸作用，产生强荧光性指纹，如图 6-3(c)所示。



(a) 碘熏法采集　　(b) 硝酸银法采集　　(c) 荧光试剂采集

图 6-3　利用化学方法采集的指纹图像

随着计算机技术、光学技术和半导体技术的发展，为克服油墨按印等物理方式采集指纹图像的缺点，发展了光学传感器、半导体传感器、超声波传感器等可以获取高质量指纹图像的采集仪。这些采集仪对获取高质量指纹图像提供了良好的技术保障，具有很高的实用价值。

同时，为了获得足够的指纹细节信息，并使指纹图像达到较高分辨率，提高指纹识别稳定性和准确性，更先进的指纹图像传感器也在研发之中。

6.2　指纹传感器的分类

指纹传感器按传感原理即指纹成像原理和技术，分为光学指纹传感器、电容指纹传感器、压感指纹传感器、热敏指纹传感器以及超声波传感器等，图 6-4 是由不同指纹传感器采集到的指纹图像。

图 6-4　不同指纹传感器采集到的指纹图像

光学指纹传感器和半导体指纹传感器是目前应用最为广泛的两类指纹传感器，同时也是最为常见的指纹传感器。超声波传感器是成像最好的传感器。下面我们将分别介绍这几种指纹传感器。

6.2.1　光学指纹传感器

光学指纹传感器是利用光学技术来采集指纹图像的传感器，如图 6-5 所示。光学指纹传感器（指纹采集仪）的出现是建立在 CCD（Charged Coupled Device）技术的基础上。20 世纪 70 年代开始，CCD 就作为感光器件被用来获取指纹图像，形成光学指纹传感器。

20 世纪 80 年代出现了光学 CMOS。和 CCD 相比，光学 CMOS 在体积、功耗和价格上具有明显优势，因此更适合用在光学指纹采集仪上。目前，几乎所有的光学指纹采集仪都采用 CMOS 感光器件。

光学指纹传感器主要是利用光的全反射原理。将手指压在棱镜电底倾斜面上时（如图 6-6 所示），在内置光源照射下，光从左侧射向棱镜电，并经棱镜电底侧射出，由 CCD 获得反射光线。反射光的数量依赖于压在玻璃表面上指纹的脊和谷的深度和皮肤与玻璃间的油脂和水分。光源射出的光线在手指表面指纹凹凸不平的线纹上折射的角度及反射的光线明暗不一样。光线经玻璃射到谷线后在玻璃与空气的界面上发生全反射，光线被反射到 CCD。但是，射向脊线的光线不发生全反射，而是被脊与玻璃的接触面吸收或者漫反射到别的地方。这样就在 CCD 上形成了脊线呈黑色、谷线呈白色的数字化的、可被指纹识别系统处理的多灰度指纹图像。

图 6-5　光学指纹采集仪

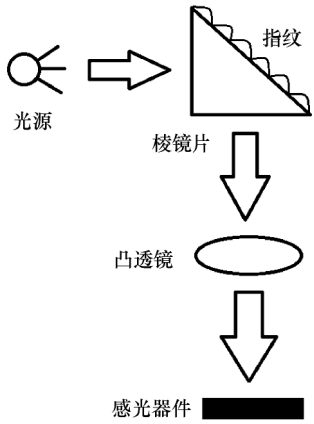


图 6-6　光学指纹传感器原理

光学指纹传感器的核心部件是电荷耦合设备（CCD），这与数码相机和摄像机中使用的光传感器系统是相同的。CCD 是一组光敏二极管，这种器件在光子的作用下可以产生电信号。每个光敏器件记录一个像素，即一个代表射中该点的光束的微小圆点。明暗像素共同构成了扫描场景（如一个手指）的图像。最后通过模数转换器，将图像的模拟电子信号转换为数字图像的形式，如图 6-7 所示。

光学传感器的优势是坚固耐用，对温度、湿度、静电都有很强的适应能力，而且成本比其它类型的指纹传感器要低，采集窗口也可以做到很大以方便使用。

光学传感器对于干手指形成的指纹图像淡而散，而对于湿手指形成的指纹图像通常会模糊。这两点都可以从光学全反射原理加以解释。由于光路部分的存在，导致光学传感器体积较大，光源和感光器件的总功耗也比较大。

为了降低功耗，减小光学传感器的体积，近年来也发展了新的技术，如利用小纤维光束来获取指纹图像。小纤维光束垂直射到指纹的表面并照亮指纹，然后通过探测指纹反射光来获取指纹图像。也有把含有一个微型棱镜片矩阵安装在指纹采集仪的弹性表面上，当手指压在此表面上时，由于指纹脊线和谷线的压力不同而改变了微型棱镜片的表面，根据棱镜片的反射光强发生变化 ，获得指纹灰度图像。

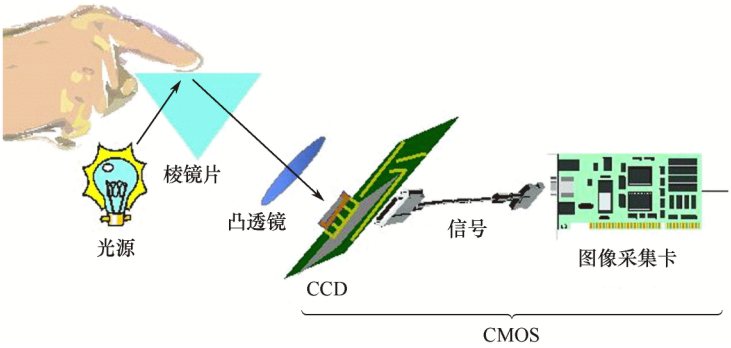


图 6-7　光学指纹传感器实际应用图

根据光学指纹传感器的特点，这类传感器比较适合用于考勤机、门锁门禁、保险柜、公安刑侦等场合。

6.2.2　半导体指纹传感器

半导体指纹传感器如图 6-8 所示，它有电容、电感、热敏和压感等传感器之分。1998 年电容式传感器面世之后，各种半导体传感器相继出现。电容指纹传感器也是半导体指纹传感器中应用最多的传感器。

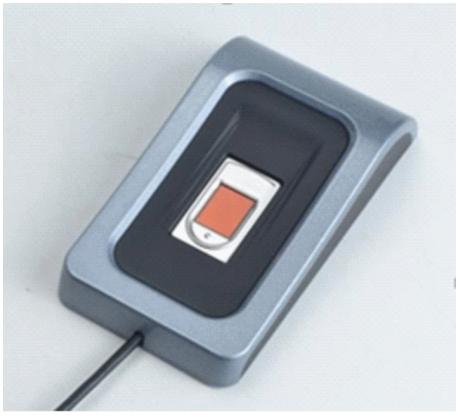


图 6-8　半导体指纹采集仪

1. 电容指纹传感器

电容指纹传感器是最常见的半导体指纹传感器。在半导体硅片表面上集成了成千上万个电容传感器，其外面是绝缘表面，当用户将手指按压在该半导体表面上时，皮肤组成了电容阵列的另一面，如图 6-9 所示。

由于手指平面由脊线、谷线构成，使得手指表面凸凹不平，凸点处和凹点处接触平板的实际距离大小就不一样，导致硅表面电容阵列的各个电容电压不同，如图 6-10 所示。通过测量并记录各点的电压值就可以获得具有灰度级的指纹图像。

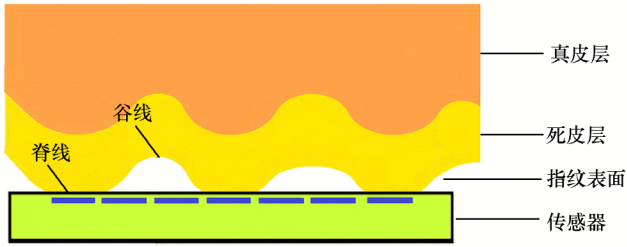


图 6-9　手指与传感器接触平面示意图

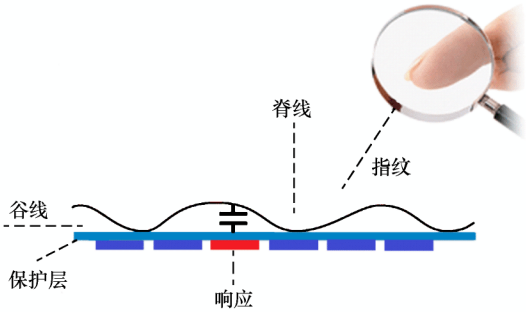


图 6-10　电容式传感器原理图

2. 压感指纹传感器

压感指纹传感器是应用压电效应来采集指纹图像的传感器。

某些电介质在沿一定方向上受到外力的作用而变形时，其内部会产生极化现象，同时在它的两个相对表面上出现正负相反的电荷。当外力去掉后，它又会恢复到不带电的状态，这种现象称为正压电效应。当作用力的方向改变时，电荷的极性也随之改变。相反，当在电介质的极化方向上施加电场，这些电介质也会发生变形。电场去掉后，电介质的变形随之消失，这种现象称为逆压电效应。依据电介质压电效应研制的一类传感器称为压感传感器。

压感指纹传感器表面的顶层是具有弹性的压感介质材料。当用户将手指按压在该半导体表面上时，这些压感介质将指纹脊线和谷线的不同压力转化为与之相应的不同电信号，并进一步产生具有灰度级的指纹图像，如图 6-11 所示。

3. 热敏指纹传感器

热敏指纹传感器是应用热敏效应来获取指纹图像的传感器。

某些材料的电阻率随温度变化而发生较明显改变，这种现象称为热敏效应。热敏式指纹传感器的表面是具有热敏效应的介质，当手指按压到传感器表面时，指纹的脊线会接触到传感器表面的介质，使介质的温度得到改变。而指纹的谷线则远离传感器表面的介质，因而谷线处的传感器的温度改变很小，甚至不发生改变，如图 6-12 所示。温度的改变使得这种介质的电阻率发生变化，进而在脊线和谷线处就会得到不同的电信号。

热敏指纹传感器就是通过感应压在半导体表面上的指纹脊线和远离半导体表面的谷线的温度不同来获得指纹图像。

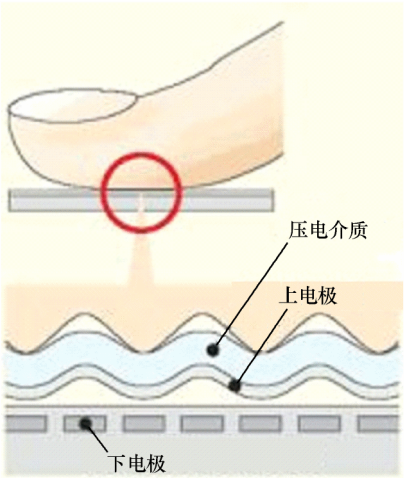


图 6-11　压感指纹传感器原理图

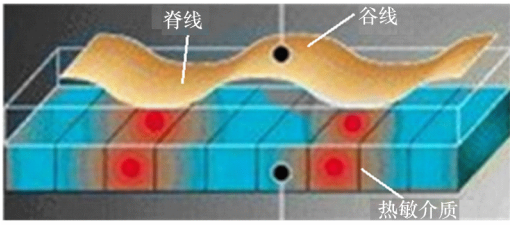


图 6-12　热敏指纹传感器

半导体指纹传感器的优点是体积小、功耗低，从图像获取能力上讲，干手指效果普遍较理想。

除了压感式传感器外，其它三种指纹传感器对湿手指进行指纹采集的效果较差。半导体指纹传感器的抗静电能力普遍较弱，容易受静电影响，甚至损坏。另外，抗磨损和抗破坏能力也远远不如光学指纹传感器。

根据半导体指纹传感器的特点，半导体指纹传感器适合用于小型、便携式设备中，如手机、U 盘、移动认证终端等。

6.2.3　超声波指纹传感器

超声波指纹传感器是利用超声波扫描技术来获取指纹图像的传感器，如图 6-13 所示。

超声波扫描技术被认为是指纹取像技术中最好的一种，但在指纹识别系统中还不多见，还处于实验室阶段。超声波指纹取像的原理是：首先用超声波对指纹的表面进行扫描，紧接着接收设备获取的反射信号。由于指纹脊线和谷线的声阻抗不同，导致反射回接收器的超声波的能量不同，测量其大小，从而产生指纹灰度图像。

超声波指纹传感器获取的是指纹真皮层的纹理信息，积累在皮肤表面上的脏东西和

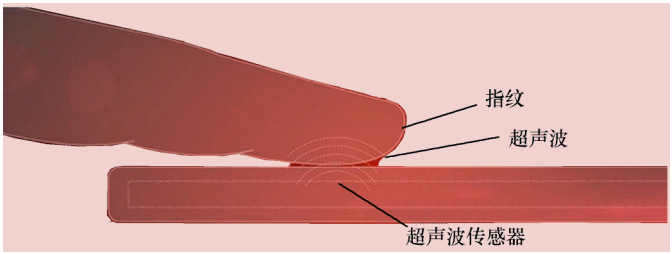


图 6-13　超声波指纹传感器

油脂对超声获取图像影响不大，所以这样获取的图像是实际指纹纹路凹凸的真实反映。

6.3　不同指纹传感器的性能比较

基于不同技术的指纹传感器都有各自的优缺点，我们通过表 6-1 来对不同的指纹传感器的性能进行比较。

表 6-1　不同指纹传感器的性能比较

性能	光学指纹传感器	半导体指纹传感器	超声波指纹传感器
成像质量	干手指成像质量差，汗多、稍脏的手指成像模糊	干手指成像质量好，汗多、稍脏的手指不能成像	非常好
成像面积	大	小	中
传感器体积	大	小	中
耐用性	非常耐用	易损坏	一般
功耗	大	小	大
价格	低	低	很高

从表 6-1 中可以看出，不同的指纹传感器的性能有一定的差距。在实际应用中，我们就可以根据实际的需求，以及不同指纹传感器的特点来选择适合我们需要的指纹传感器。

6.4　本章小结

本章首先简单介绍了指纹图像采集的发展历史，然后分别介绍了光学指纹传感器、半导体指纹传感器以及超声波指纹传感器的原理，最后对比了几种指纹传感器的性能。

随着科学技术的发展，以及指纹识别技术的广泛应用，新型的指纹传感器也在研究之中。指纹传感器也必定向着尺寸更小、分辨率更高、抗噪能力更强、防伪能力更好以及成本更低的方向快速发展。

习题与思考题

1. 指纹图像采集的方式有哪些？在日常生活中，你接触到的采集方式有哪些？
2. 指纹传感器分为几类，每一类指纹传感器的优缺点是什么？

3. 影响采集的指纹图像的质量的因素有哪些？哪个因素对指纹图像的质量的影响最大？
4. 简述光学指纹传感器的原理。
5. 简述电容指纹传感器的原理。
6. 简述超声波指纹传感器的原理。
7. 你认为什么新技术可以被应用到指纹传感器的设计中？如果让你设计一个指纹传感器，你将如何设计？

第 7 章　指纹图像分割

在指纹采集过程中，采集到的指纹图像常常含有大量包含噪声的干扰区域，如现场指纹中的复杂背景。这些干扰区域通常不会含有有效的指纹信息，需要去除干扰区域才能对采集到的指纹图像进行有效地增强并减少在此过程中的计算量。

指纹图像分割作为预处理的第一步，它的主要目的是使前景区域与背景区域分离开来，并丢弃背景区域以减少错误特征的数量。

本章内容：7.1 节介绍指纹分割的原因、目的和本质，7.2 节介绍指纹分割指标的计算，7.3 节介绍用于指纹分割的最小均方算法，7.4 节介绍用于指纹分割的聚类算法，7.5 节总结本章的内容。

7.1　指纹分割概述

在实际采集指纹过程中，由于采集仪器表面、指纹皮肤的洁净程度以及采集设备本身的影响等，使得采集到的图像中含有大量的噪声，甚至畸变。尤其采集现场指纹时，指纹图像的背景区域对于后续的指纹识别毫无帮助，甚至会导致错误匹配。因此，在对指纹图像进行增强之前，应对指纹图像进行指纹图像分割。

指纹图像分割的主要任务是分割出指纹图像中的前景区域（指纹区域）及背景区域（非指纹区域），使后续的处理避免背景区域的噪声污染，只针对前景区域，以利于提高整个系统的识别速率和准确性。

目前，现有的主流指纹图像分割方法是将整幅指纹图像划分为一系列互不重叠的小块，然后对每一个小块提取若干特征，最后通过融合已提取的特征来判断每个小块是属于前景区域还是背景区域。还有其它的指纹图像分割方法是将每个像素看作一个小块，然后计算每个像素的一些特征并依此来分割指纹图像。

基于对现有指纹图像分割方法的分析及指纹图像分割本质的认识，可以将指纹图像分割看成一个两类别（即前景区域类别和背景区域类别）分类问题。对于一个分类问题，其分类的效果完全取决于分类特征的提取以及分类算法的选择，其中，分类特征的提取起着至关重要的作用，提取出具有较强鉴别能力的特征往往会使整个分类工作起到事半功倍的效果。

后续内容详细介绍了利用分类特征对指纹进行分割的方法，并从指纹分割的步骤展开，细分为三个部分：分割指标选取、利用最小均方算法进行权重的分配和利用聚类算法判断像素是否属于前景区域。

7.2　指纹分割指标计算

指纹分割指标是指前景区域和背景区域之间普遍具有差别的指纹图像像素特征。灰

度值统计特征(如灰度均值、灰度方差等)、局部方向性特征(如方向一致性等)和纹线特征(如脊线频率等)均可作为指纹分割特征的图像特征。

这些图像特征可以单独用作指纹分割的依据,也可以通过计算权重的方法来对多种特征进行融合,最后获得一个融合阈值进行指纹分割。指纹分割方法中较为常用的指纹图像像素特征为灰度均值、方差和方向一致性。下面详细介绍这三种指纹图像特征。

1. 灰度均值

灰度均值(Mean)可以作为指纹图像分割的像素特征的原因是:对于大多数指纹采集设备来说,在成像过程中,与传感器表面接触的指纹部分形成黑、白交替的指纹图像,而没有接触的部分,则形成偏白的背景区域。因此,可以利用前景区域的灰度均值小于背景区域这一特征来分割指纹图像。

灰度均值的计算公式为:

$$\text{mean} = \frac{1}{S}\sum_{(x,y)\in W} I(x,y) \tag{7-1}$$

式中,W 表示当前块;S 表示当前块的大小;$I(x,y)$表示点(x,y)处的灰度值。

如图 7-1 所示,对于前景区域和背景区域灰度值相差较大的指纹图像,单独使用灰度均值作为指纹图像分割指标的效果更好。

(a)原始图像　　(b)分割后的结果图

图 7-1　对质量较好指纹图像使用灰度均值分割

但是,在实际采集过程中,由于指纹的按压力度、干湿度及背景光线等因素的影响,使得采集到的一些指纹图像的前景区域和背景区域灰度值较为接近。如图 7-2(a)所示,从该图可以直观地看出前景区域和背景区域的灰度均值较为接近,而从图 7-2(b)可以看出,单独使用指纹灰度均值作为指纹图像分割指标很难将其前景区域和背景区域分割开来。

2. 方差

方差(Variance)是描述图像信息的重要特征,图像的方差能够较好地体现图像的细节信息,它与高频部分有关,而图像的高频部分也是人眼较为敏感的内容。

方差作为分割指纹图像的依据,在指纹的前景区域,由于脊线和谷线的交替变化,使得图像中的灰度变化较为急剧,灰度方差的值偏大;而在背景区域,由于在成像时就没有和指纹接触过,因此灰度较为单一,变化相对缓慢,灰度方差值偏小。

(a)原始指纹图像　　(b)分割后的结果图

图 7-2　灰度均值分割后的结果图

方差的计算公式如下：

$$\mathrm{Var}=\frac{1}{S}\sum_{(x,y)\in W}(I(x,y)-\mathrm{mean})^2 \tag{7-2}$$

式中，W 表示当前块；S 表示当前块的大小；$I(x,y)$表示点(x,y)处的灰度值；mean 表示当前块中的灰度均值。

如图 7-3 所示，对于背景区域受噪声污染较轻的指纹图像，单独使用方差作为指纹分割指标的效果较好。

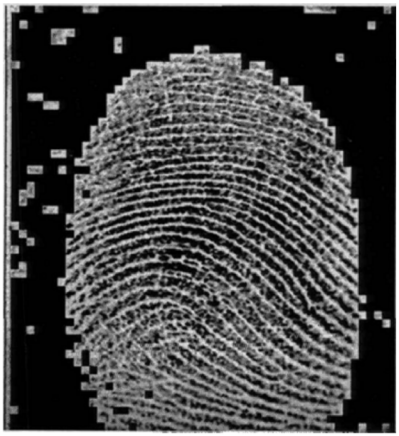
(a)原始图像　　(b)分割后的结果图

图 7-3　对质量较好指纹图像使用灰度方差分割

从式(7-2)可以明显看出该特征对灰度变化较为敏感，但是在指纹图像的实际采集过程中，由于采集头表面和指纹皮肤的洁净程度以及采集设备本身的影响等，采集得到的图像中含有大量的噪声，这些噪声使得指纹图像中背景区域处的灰度方差值也偏大，增加了利用该特征分割指纹图像的难度。

图 7-4 给出了一幅受噪声污染较为严重的指纹图像，同时给出了使用灰度方差分割后的结果图，从分割结果中可以看出，在背景区域中，有些区域受噪声影响较大，使得该区

(a)原始图像



(b)分割后的结果图

图 7-4　灰度方差分割后的效果图

域内的灰度方差值亦较大,从而被误分割为前景区域。

3. 方向一致性

方向一致性(Coherence)是评价同一方向上梯度作用效果的参数,它反映了一个块的方向强度的大小。由于指纹前景区域是具有方向信息的物理图像其方向一致性称好,而背景区域则没有处理信息,方向一致性称差,所以方向一致性可以作为指约分割的指标。

方向一致性的计算公式如下:

$$\mathrm{Coh}=\frac{\left|\sum\limits_{(x,y)\in W}\left[G_{sx}(x,y),G_{sy}(x,y)\right]\right|}{\sum\limits_{(x,y)\in W}\left|G_{sx}(x,y),G_{sy}(x,y)\right|} \tag{7-3}$$

其中

$$\begin{bmatrix}G_{sx}(x,y)\\G_{sy}(x,y)\end{bmatrix}=\begin{bmatrix}G_x^2(x,y)-G_y^2(x,y)\\2G_x(x,y)G_y(x,y)\end{bmatrix} \tag{7-4}$$

$$\left[G_x(x,y),G_y(x,y)\right]^{\mathrm{T}}=\left[\frac{\partial I(x,y)}{\partial x},\frac{\partial I(x,y)}{\partial y}\right]^{\mathrm{T}} \tag{7-5}$$

在式(7-3)、式(7-4)和式(7-5)中,(G_{sx},G_{sy})是平方梯度,$G_{xx}=\sum_W G_x^2$,$G_{yy}=\sum_W G_y^2$,$G_{xy}=\sum_W G_xG_y$;(G_x,G_y)是局部梯度。其中,W 为当前块。

如图 7-5 所示,对于背景区域受噪声污染较轻的指纹图像,单独使用一致性作为指纹分割指标的效果更好。

方向一致性反映了在一个局部小块内所有点的梯度方向一致性程度,当块内所有点都指向同一个方向时,此时的方向一致性程度最高,值为 1;当块内所有点的方向均匀分布在各个方向时,一致性最低,值为 0;其它情况下,一致性特征的取值介于 0 和 1 之间。

方向一致性相对于灰度均值和方差两种特征,最大的优势在于把握住了指纹图像是一种具有方向性的纹理图像这一本质,因此,该特征的针对性较强。但是该特征也有其自身的缺陷:指纹的中心点区域由于纹线走向变化较为急剧,使得该处的一致性较低,容易

(a)原始图像

(b)分割后的结果图

图 7-5　一致性分割后的效果图

被误分割为背景区域;另外,当指纹的前景区域受到噪声影响后,此时计算出的方向一致性的值也偏低,容易产生误分割。

(a)原始图像　　(b)分割后的结果图

图 7-6　方向一致性分割后的效果图

如图 7-6 所示,给出了一幅受噪声污染较为严重的指纹图像,同时给出了使用方向一致性分割后的结果图。从图 7-5(b)中可以看出,在指纹的中心区域,方向变化较大的块被误分为背景区域,其余的前景及背景区域,由于受噪声影响,也产生了大量的误分割。

7.3　最小均方算法用于指纹分割

7.2 节介绍了可以用于区分指纹图像前景区域和背景区域的几种指纹图像特征。由于单独使用灰度均值、方差和方向一致性进行指纹图像分割的局限性较大,因此,下面介绍一种将它们融合起来形成一个综合阈值的方法——最小均方算法。

最小均方算法(Least mean square,LMS)是一种最简单、应用最为广泛的自适应滤波

算法，是基于最小均方误差准则（Minimum Mean Square Error，MMSE）的维纳滤波器，运用最速下降法后的优化延伸。最早是由 Widrow 和 Hoff 于 1967 年提出来的，因此这种算法也被称为 Widrow-Hoff LMS 算法。

最小均方算法在自适应滤波器中得到广泛应用，在指纹分割中的作用是在多特征融合阈值时通过该算法训练产生各特征的权重值。

自适应滤波算法从某种角度也被称为性能表面搜索法，在性能表面中，它是通过不断测量一个点是否接近目标值，来寻找最优解的。目前，使用最为广泛的曲面函数之一是均方误差（Mean Square Error，MSE）函数，函数表达式如下：

$$f(e(k))=\xi(k)\triangleq E\{|e(k)|^2\} \tag{7-6}$$

式中，$e(k)$表示误差信号；$E\{\cdot\}$表示对信号的空间集取期望。根据自适应滤波器的结构图（如图 7-6 所示），$e(k)$是滤波器期望信号和滤波器输出信号之间的差，即

$$e(k)=d(k)-y(k) \tag{7-7}$$

直接型有限长单位冲激响应（Finite Impulse Response，FIR）横向滤波器的结构如图 7-7 所示。输入信号为 $x(k)$，即输入信号 $x(k)$经过 L 个延时器后，在 k 时刻形成的信号矢量，$\boldsymbol{x}(k)=[x(k),x(k-1),\cdots,x(k-L+1)]^{\mathrm{T}}$，$w_i(k)$为第 $i+1$ 个延时单元的抽头系数，$\boldsymbol{w}(k)=[w_0(k),w_1(k),\cdots,w_{L-1}(k)]^{\mathrm{T}}$。

输出信号为

$$y(k)=\sum_{n=0}^{n=L-1} w_i(k)x(k-n)=\boldsymbol{w}^{\mathrm{T}}(k)\boldsymbol{x}(k) \tag{7-8}$$

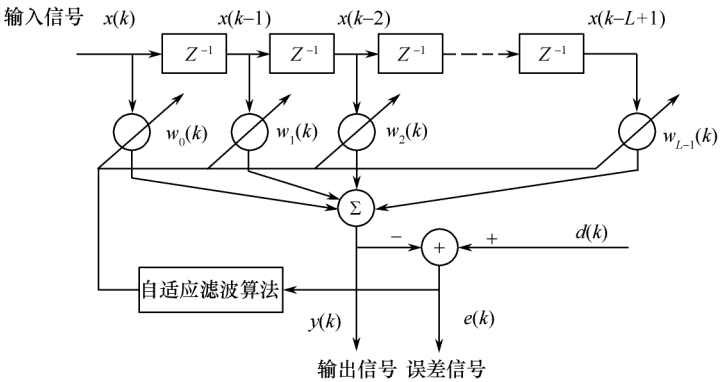


图 7-7　自适应滤波器结构图

将式(7-8)代入表达式(7-7)中，得：

$$e(k)=d(k)-\boldsymbol{w}^{\mathrm{T}}(k)\boldsymbol{x}(k) \tag{7-9}$$

准则函数设计为求均方误差函数的最小值，我们称之为最小均方误差准则（MMSE），维纳滤波器就是基于这个准则推导出来的。

把式(7-9)代入式(7-6)，展开得到

$$\xi(k)=E\{d(k)^2\}+\boldsymbol{w}^{\mathrm{T}}(k)E\{\boldsymbol{x}(k)\boldsymbol{x}^{\mathrm{T}}(k)\}\boldsymbol{w}(k)-2E\{\boldsymbol{x}^{\mathrm{T}}(k)d(k)\}\boldsymbol{w}(k) \tag{7-10}$$

$$=E\{d(k)^2\}+\boldsymbol{w}^{\mathrm{T}}(k)\mathbf{R}\boldsymbol{w}(k)-2\mathbf{P}^{\mathrm{T}}\boldsymbol{w}(k) \tag{7-11}$$

式中，$\boldsymbol{P}$ 和 $\boldsymbol{R}$ 分别表示滤波器输入信号 $x(k)$ 与期望信号 $d(k)$ 的互相关矩阵和滤波器输入信号 $x(k)$ 的自相关矩阵，$\boldsymbol{P}$ 和 $\boldsymbol{R}$ 的表达式分别如式(7-12)和式(7-13)所示。

$$\boldsymbol{P}=E\{x(k)d(k)\}=\begin{bmatrix} d(k)x(k) \\ d(k)x(k-1) \\ \cdots \\ d(k)x(k-L+1) \end{bmatrix} \tag{7-12}$$

$$\begin{aligned}\boldsymbol{R}&=E\{x(k)x^{\mathrm{T}}(k)\}\\&=E\begin{bmatrix} x(k)x(k) & x(k)x(k-1) & \cdots & x(k)x(k-L+1) \\ x(k-1)x(k) & x(k-1)x(k-1) & \cdots & x(k-1)x(k-L+1) \\ \cdots & \cdots & & \cdots \\ x(k-L+1)x(k) & x(k-L+1)x(k-1) & \cdots & x(k-L+1)x(k-L+1) \end{bmatrix}\end{aligned} \tag{7-13}$$

在上式中，若假设 k 是一个固定值，ξ_k 可以认为是一个和时间无关的函数，则式(7-11)可以写成为：

$$\xi=E\{d(k)^2\}+\boldsymbol{w}^{\mathrm{T}}\boldsymbol{R}\boldsymbol{w}-2\boldsymbol{P}^{\mathrm{T}}\boldsymbol{w} \tag{7-14}$$

从上式可以看出均方误差 ξ 与滤波器权向量 $\boldsymbol{w}$ 是成二次函数关系，引入均方误差曲面来描述函数的映射关系，对应的权向量 $\boldsymbol{w}$ 的二次函数就是一个超抛物曲面。图 7-8 是一个只含两个值的权向量的均方误差曲面。

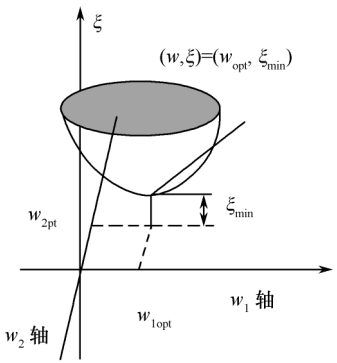


图 7-8　权向量阶数为 2 的均方误差曲面

从图 7-8 中可以明显发现，曲面存在且只有唯一的最小值，位于曲面最底部，根据最小均方误差准则，设计的滤波器就是找到这个最小值的对应权向量，也就是均方误差在权向量面上的投影，我们对代价函数中的 $\boldsymbol{w}$ 求导数，可得：

$$g=\partial\xi/\partial\boldsymbol{w}=2\boldsymbol{R}\boldsymbol{w}-2\boldsymbol{P} \tag{7-15}$$

输入信号 $x(k)$ 的功率谱密度存在非零频率，所以自相关矩阵 $\boldsymbol{R}$ 是正定矩阵也就是非奇异矩阵，令 $\boldsymbol{g}$ 的值为零，则得到使均方误差函数最小的滤波器权向量

$$\boldsymbol{w}_{\mathrm{opt}}=\boldsymbol{R}^{-1}\boldsymbol{P} \tag{7-16}$$

最小均方误差值：

$$\xi_{\min}=E\{d(k)^2\}+\boldsymbol{w}_{\text{opt}}\boldsymbol{R}\boldsymbol{R}^{-1}\boldsymbol{p}-2\boldsymbol{w}_{\text{opt}}^{\mathrm{T}}\boldsymbol{p}=E\{d(k)^2\}-\boldsymbol{w}_{\text{opt}}^{\mathrm{T}}\boldsymbol{p} \tag{7-17}$$

式(7-16)就是 Widrow-Hoff 方程的最优权向量，即维纳解，将该解作为最优滤波器权系数的线性滤波器，我们称之为维纳滤波器。

由于输入信号和噪声信号的统计特性常常是很难获得的，因此也就很难准确求出输入信号的自相关矩阵 $\boldsymbol{R}$ 和互相关向量 $\boldsymbol{p}$，还需要对矩阵进行求逆运算。因此，我们在设计滤波器时引入梯度算法，给权向量 $\boldsymbol{w}_k$ 一个初始值，一般取值为零，然后通过最小化均方误差函数，在均方误差曲面上不断调节更新，直到达到最小均方误差的点，该点在权向量平面上的投影，就是维纳解 $\boldsymbol{w}_{\text{opt}}$，或者是在它的某一个邻域。

根据最小均方误差准则以及均方误差曲面，我们自然地会想到沿每一时刻均方误差的最速下降在权向量面上的投影方向更新，也就是通过目标函数 ξ_k 的反梯度向量来反复迭代更新。由于均方误差性能曲面只有一个唯一的极小值，只要收敛步长选择恰当，不管初始权向量在哪，最后都可以收敛到误差曲面的最小点，或者是在它的一个邻域内。这种沿目标函数梯度反方向来解决最小化问题的方法，我们一般称为最速下降法，表达式如下：

$$w(k+1)=w(k)+\frac{1}{2}\mu(-\nabla_k) \tag{7-18}$$

式中，k 表示迭代时刻，μ 是控制算法收敛速度和稳定性的步长参数，$\boldsymbol{\nabla}_k$ 表示目标函数的梯度向量，其表达式如下：

$$\boldsymbol{\nabla}_k=\nabla E\{e^2(k)\}=\partial\xi(k)/\partial w(k)=2\boldsymbol{R}\boldsymbol{w}(k)-2\boldsymbol{P} \tag{7-19}$$

将式(7-19)代入式(7-18)，可得滤波器权向量更新表达式如(7-20)所示。

$$w(k+1)=w(k)+\mu(\boldsymbol{p}-\boldsymbol{R}w(k)) \tag{7-20}$$

通过式(7-20)虽然避免了维纳滤波要对自相关矩阵 $\boldsymbol{R}$ 的求逆，但是要精确地计算其梯度 $\boldsymbol{\nabla}_k$ 是十分困难的，因为其自相关矩阵 $\boldsymbol{R}$ 和互相关向量 $\boldsymbol{p}$ 在没有先验信息的情况下很难得到，一种粗略的又简单有效的计算方法是：直接用 k 时刻瞬时误差的平方 $e^2(k)$ 取代均方误差 $E\{e^2(k)\}$ 作为求梯度 $\boldsymbol{\nabla}_k$ 的估计，即

$$\boldsymbol{\nabla}_k\approx\partial e^2(k)/\partial w(k)=-2e(k)x(k) \tag{7-21}$$

用式(7-21)代替式(7-19)的 $\boldsymbol{\nabla}_k$，得到基于随机梯度下降法的自适应 LMS 算法数学表达式如(7-22)所示。

$$w(k+1)=w(k)+\mu e(k)x(k) \tag{7-22}$$

把式(7-22)，式(7-8)和式(7-7)联立起来，可得基于随机梯度算法的最小均方自适应滤波算法的完整表达式如(7-23)所示。

$$\begin{cases}y(k)=w^{\mathrm{T}}(k)x(k)\\ e(k)=d(k)-y(k)\\ w(k+1)=w(k)+\mu e(k)x(k)\end{cases} \tag{7-23}$$

LMS 自适应算法是一种特殊的梯度估计，不必重复使用数据，也不必对相关矩阵 $\boldsymbol{R}$ 和互相关矩阵 $\boldsymbol{P}$ 进行运算，只需要在每次迭代时利用输入向量和期望响应，结构简单，易于实现。但是精确分析最小均方算法的收敛过程和性能却是非常困难的，因而一直是个

热门的研究方向。

7.4 用于指纹分割的聚类方法

在7.3节中讲述了使用最小均方算法训练权重值，并用线性分类器对指纹图像中的像素进行分类。而在这个过程中会产生错误，如将背景区域的像素错分成前景区域的像素或将前景区域的有效像素归纳为背景区域的像素。因此，本节将详细介绍一种修正这些错误划分的方法——聚类方法。

聚类是一个将数据集划分为若干组或类的过程，并使得同一组内的数据对象具有较高的相似度，而不同组中的数据对象是相异的。除了在图像分割方面的应用，聚类算法还可以用于数据分析，数据挖掘，统计学和机器学习等领域。聚类算法的种类也很多样，下面就介绍几种常用聚类算法。

7.4.1 K-均值算法

K-均值(K-MEANS)聚类算法是由美国J. B. MacQueen教授于1967年提出的一种聚类算法，它是聚类分析方法中一种基本的且应用最广的划分方法。因该算法具有简单快速、适于处理大数据集等优点，目前，已被广泛应用于科学研究和工业应用。

K-均值聚类算法是一种典型的基于距离的硬聚类算法，算法通常采用误差平方和函数作为优化的目标函数，误差平方和函数的定义式如下。

$$E=\sum_{j=1}^{K}\sum_{x\in C_j}\|x-m_j\|^2 \tag{7-24}$$

其中，K 表示聚类的数目；$C_j(j=1,2,\cdots,K)$ 表示聚类的第 j 个簇；x 表示簇 C_j 中的任意数据对象；m_j 表示簇 C_j 的均值。E 表示数据样本与簇中心间差异度平方之和，E 值的大小取决于 K 个聚类中心点。E 值越小，聚类结果的质量就越好。因此，我们应该设法找到使聚类准则函数 E 的值达到最小的聚类结果。

K-均值算法的基本思想是首先从含有 n 个数据对象的数据集中随机选择 K 个数据对象作为初始中心，然后计算每个数据对象到各中心的距离，根据最近邻原则，所有数据对象将会被划分到离它最近的那个中心所代表的簇中，接着分别计算新生成的各簇中数据对象的均值作为各簇新的中心，比较新的中心和上一次得到的中心。如果新的中心没有发生变化，则算法收敛，输出结果；如果新的中心和上一次的中心相比发生变化，则要根据新的中心对所有数据对象重新进行划分，直到满足算法的收敛条件为止。

K-均值聚类算法的主要工作流程可以用图7-9表示。

K-均值聚类算法的优点是过程简单易理解、快速有效、适于处理大数据集等，但是其自身仍然存在一些不足和缺陷，如K-均值聚类算法对初始中心点的选取非常敏感，算法易陷入局部最优解，通常难以发现球状簇以外的其它形状的簇，而且聚类数目 K 的值通常需要用户事先给定等，在一定程度上限制了它的应用和发展。

该算法的伪代码如下：

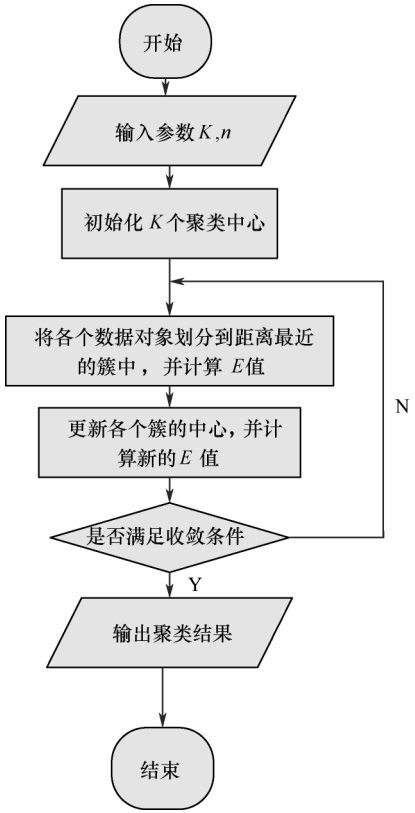


图 7-9　K-均值聚类算法流程图

Procedure K—MEANS

Input:S=$\{X_1, X_2, \cdots, X_n\}$

Output:k cluster centers,k cluster set C_j

Begin

m=1

Initialize k prototypes $Z_j, j \in [1,k]$

Repeat

For i=1 to n do

Begin

For j=1 to k do

Compute $D(X_i, Z_j) = |X_i - Z_j|$

If $D(X_i, Z_j) = \min\{D(X_i, Z_j)\}$ then $X_i = \in C_j$

End

If m=1 then $J_c(m) = \sum_{j=1}^{k} \sum_{X_j \in C_j} |X_i - Z_f|^2$

m=m+1

For j=1 to k do

$$Z_j = \frac{1}{n}\sum_{i=1}^{n} X_i^{(j)}$$

$$J_c(\mathrm{m}) = \sum_{j=1}^{k}\sum_{X_i \in C_j} |\ X_i - Z_j\ |^2$$

Until$|J_c(\mathrm{m}) - J_c(\mathrm{m}-1)| < \xi$

End

7.4.2 层次聚类算法

层次聚类方法是根据给定的簇间距离度量准则，构造和维护一棵由簇和子簇形成的聚类树，直至满足某个终结条件为止。根据层次分解是自底向上还是自顶向下形成，层次聚类方法可以分为凝聚的(agglomerative)和分裂的(divisive)。一个纯粹的层次聚类方法的聚类质量受限于如下特点：一旦一个合并或分裂执行，就不能修正。

凝聚的层次聚类：这种自底向上的策略首先将每个对象作为一个簇，然后合并这些原子簇为越来越大的簇，直到所有的对象都在一个簇中，或者某个终结条件被满足。绝大多数层次聚类方法属于这一类，它们只是在簇间相似度的定义上有所不同。

分裂的层次聚类：这种自顶向下的策略与凝聚的层次聚类相反，它首先将所有对象置于一个簇中，然后逐步细分为越来越小的簇，直到每个对象自成一簇，或者达到了某个终结条件，例如达到了某个希望的簇数目，或者两个最近的簇之间的距离超过了某个阈值。

图 7-10 中，描述了一个凝聚的层次聚类方法 AGNES(Agglomerative NESting)和一个分裂的层次聚类方法 DIANA(Divisive ANAlysis)在一个包含 5 个对象的数据集合{a，b，c，d，e}上的处理过程。最初，AGNES 将每个对象作为一个簇，然后这些簇根据某些准则被一步步地合并。例如，如果簇 C_1 中的一个对象和簇 C_2 中的一个对象之间的距离是所有属于不同簇的对象之间的距离欧氏距离中最小的，C_1 和 C_2 可能被合并。这是一种单链

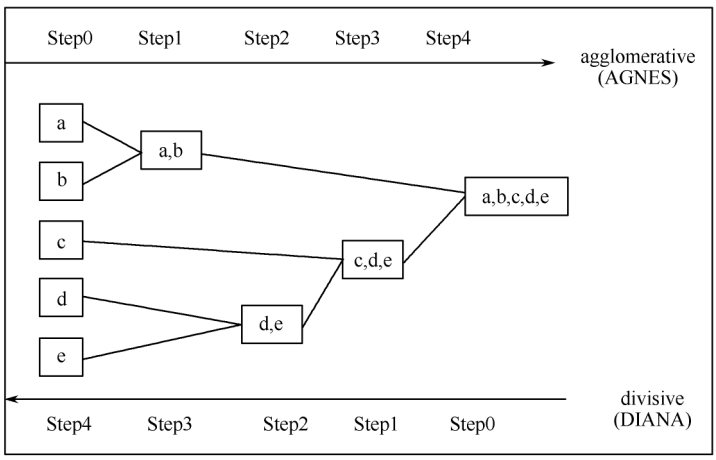


图 7-10 凝聚和分裂层次聚类

接(Single-link)方法,其每个簇可以被簇中所有对象代表,两个簇间的相似度由这两个不同簇中距离最近的数据点对的相似度来确定。聚类的合并过程反复进行直到所有的对象最终合并形成一个簇。在 DIANA 方法的处理过程中,所有的对象初始都放在一个簇中。根据一些原则(如簇中最临近对象的最大欧氏距离),将该簇分裂。簇的分裂过程反复进行,直到最终每个新的簇只包含一个对象。在凝聚或者分裂的层次聚类方法中,用户能定义希望得到的簇数目或者定义阈值等方法作为结束条件。

层次聚类算法的困难在于合并或分裂点的选择。这是非常关键的,因为一旦一组对象被合并或者分裂,下一步的处理将在新生的簇上进行。已做的处理不能被撤销,聚类之间也不能交换对象。如果在某一步没有很好地选择合并或分裂的决定,可能会导致低质量的聚类结果。而且,这种聚类方法不具有很好的可伸缩性,因为合并或分裂的决定需要检查和估算大量的对象或簇。

该算法的伪代码如下:

```
Procedure AGNES
  Input:the goal unmber of cluster K,sample set D[a,b,c,d...]
  Output:K sets of cluster
        clusters←a,b,c,d...
        Compute the distance between different clusters
        Merge into one cluster←clusters of the minimum distance
        counter←counter+1
        While(counter<K)
          Repeat 5-7
        Else
        End while
```

以上介绍了将多种指纹图像特征融合的最小均方算法以及修正分类错误的聚类算法,图 7-11 显示了基于一致性、均值和方差的多特征融合分割算法的效果图。

将图 7-11 与 7.2 节的图 7-2、图 7-3 和图 7-5 相比较后可以看出,利用多种特征融合得到的阈值进行分割,能将原图中的背景区域和前景区域很好的分开,尤其是中心区域和部分边缘区域。但是,仍有一些边缘区域被误分为背景区域,从而被舍弃。

每种分割方法都有它的局限性,对于不同的指纹图像进行分割时,要根据该指纹图像的特点来选择合适的指纹图像分割算法。

该算法的伪代码如下:

```
Procedure Segmentation
  Input:Original image I
  Output:Segmented image I'
  Denote M,Coh and Var as mean, coherence and variance of all pixels gray value in I
    For each pixel (i,j) in I do
    If i∈((N+1)/2 : (a-(N-1))/2) and j∈((N+1)/2 : (b-(N-1))/2) then
Mean(i,j) = ∑_M I
```

$Var(i,j)=\sum_{M}(\mathrm{I}-mean)^2$

$Coh(i,j)=\frac{\sqrt{(G_{xx}-G_{yy})^2+4G_{xy}^2}}{G_{xx}+G_{yy}}$

Else

$Mean(i,j)=0$

$Var(i,j)=0$

$Coh\ \ (i,j)=0$

End If

End for

For each pixel (i,j) in I do

$V(i,j)=W^{\mathrm{T}}X$

If $V(i,j)>0$ Then

$Isfore(i,j)=1$

Else

$Isfore(i,j)=0$

End if

End for

(a) 原图

(b) 分割后的图像

图 7-11　使用多特征阈值分割算法

7.5　本章小结

本章首先介绍了指纹图像分割的重要性，然后从指纹分割指标计算、最小均方算法和聚类算法三个方面详细介绍了一个多特征阈值融合指纹分割算法的流程，最后通过对指纹图像的分割效果图来展示该算法的作用。

指纹分割算法还有很多其它的方法，如采用分级分割的方法，以及采用其他新的特征进行分割的方法。本书讲述了较为经典的指纹图像分割算法，其它的指纹分割算法可以自己进一步学习。

习题与思考题

1. 除了书中介绍的灰度均值、方向一致性和方差之外，你认为还有什么指纹图像特征可以作为指纹图像分割指标？
2. 比较均值、方差和一致性对指纹图像分割效果的影响并思考原因。
3. 编写使用均值或方差或一致性进行指纹分割的程序。验证习题 2 中的答案是否正确。
4. 指纹分割的作用是什么？是否可以应用于其它领域？

第 8 章　指纹图像增强与二值化

因为指纹本身或者仪器采集的原因，通常采集到的指纹存在着大量噪声，因此指纹图像分割之后，需要对指纹的有效区域进行图像增强。指纹图像增强，就是对指纹图像采用一定的算法进行处理，使其纹线结构清晰化，尽量突出和保留固有的特征信息，而避免产生伪特征信息。

图像增强之后，为了后续的特征提取，还需要对图像进行二值化的操作。图像二值化则是在增强的图像基础上，将 256 个亮度等级的灰度图像通过适当的阈值选取，获得仍然可以反映图像整体和局部特征的二值化图像，从而为识别算法的特征提取做准备。

本章内容：8.1 节介绍多种指纹图像的增强算法，8.2 介绍基于 Gabor 滤波的增强算法，8.3 节介绍基于方向各向异性滤波的增强算法，8.4 介绍对增强后的的指纹图像的二值化，8.5 节总结本章的内容。

8.1　增强

指纹图像增强的算法有很多种，比如基于 Gabor 滤波的增强算法、基于傅里叶滤波的低质量指纹增强算法、基于知识的指纹图像增强方法、非线性扩散模型及其滤波方法、多尺度滤波方法等。

基于 Gabor 滤波的增强算法的基本出发点是基于指纹的数学模型，指纹在局部小区域内可以认为是一组平行的具有一定频率的直线，那么可以顺着脊线的方向使用 Gabor 窗函数去过滤图像，使脊线的信息得到加强；基于傅里叶滤波的算法是通过傅里叶变换把指纹图像增强从空域转化为频域，然后在频域上对指纹图像进行带通滤波、方向滤波，从而使指纹图像得到增强；基于知识的指纹图像增强算法的核心思想是用计算机来模拟人工做图像增强的做法，利用两方面的先验知识对指纹图像进行增强，一是指纹的脊线在一个较小的局域内可以用低次曲线拟合，二是指纹图像中脊线和谷线互相交替出现且宽度大致相等；非线性扩散模型的滤波方法则是利用非线性扩散模型对指纹图像进行建模，利用其相应理论对指纹图像进行滤波增强；多尺度滤波是在指纹增强中引入了多尺度空间理论，合理组织这些不同尺度的信息，进而利用和分析不同尺度的信息，最终实现对指纹图像的增强。

在这里，我们详细介绍基于 Gabor 滤波的增强算法，并与之比较，再简单介绍一种利用方向各向异性椭圆滤波器进行增强的方法。基于 Gabor 滤波的增强算法包含了归一化、方向图、频率图、区域 Mask、滤波 5 个部分，而基于方向各向异性滤波器的增强算法则是在指纹图像归一化和求取方向图之后，直接利用方向图的信息进行滤波。

归一化是为了增大指纹脊线与谷线的对比度；方向图是在归一化图像的基础上，求取脊线的方向场，即脊线的走向；而频率图则是在每个块的方向场（方向图中会介绍“块”的概念）上建立坐标系，从而进一步计算脊线的频率；区域 Mask 就是对指纹进行分割，划分

有效区域和无效区域，选择质量相对较好的指纹图像进行滤波；Gabor 滤波则是利用 Gabor 滤波器对指纹进行滤波，其中上述所求的方向场、频率场，分别作为 Gabor 滤波器的方向参数和频率参数。

基于 Gabor 滤波增强算法的流程图，如图 8-1 所示。

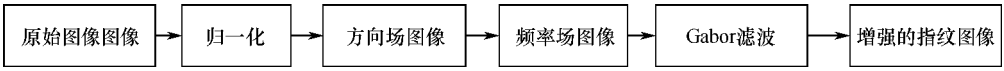


图 8-1　基于 Gabor 滤波增强算法流程图

8.2　基于 Gabor 滤波的增强算法

基于 Gabor 滤波的增强算法是指纹图像增强算法中最为经典的一种，许多其它的增强算法都是基于 Gabor 滤波增强算法演变而来。下面详细介绍 Gabor 滤波算法的各个步骤。

8.2.1　归一化

对原指纹图像进行归一化操作是指纹图像增强的第一步。归一化就是通过数学运算的方法让处理后的图像达到一个预设的均值和方差。指纹图像归一化处理的目的是降低指纹脊线和谷线间的灰度偏差，使后续操作具有统一的基准。当然，灰度图像归一化并不改变指纹纹理的清晰度。

归一化操作公式如下所示。

$$G(i,j)=\begin{cases} M_0+\sqrt{\dfrac{\mathrm{VAR}_0(I(i,j)-M(I))^2}{\mathrm{VAR}}}, & I(i,j)>M \\ M_0-\sqrt{\dfrac{\mathrm{VAR}_0(I(i,j)-M(I))^2}{\mathrm{VAR}}}, & \text{其它} \end{cases} \tag{8-1}$$

其中，$I(i,j)$表示像素点(i,j)的灰度值；M_0和 VAR_0分别表示 I 的均值和方差；$G(i,j)$表示像素点(i,j)归一化以后的灰度值。

对指纹图像归一化的前后效果对比，如图 8-2 所示。从图中可以看到归一个后，图像的对比度明显增大。

伪代码如下：

```
m=mean(Image I(x,y));
v=variance(Image I(x,y));
for every coordinate (x,y)
    if I(x,y)>m
    N(x,y)=m0+sqrt{[v0*(I(x,y)-m)^2]/v};
    else
    N(x,y)=m0-sqrt{[v0*(I(x,y)-m)^2]/v};
```

(a) 指纹原图像　　(b) 指纹归一化图像

图 8-2　指纹归一化效果对比图

8.2.2　方向图

正如算法介绍中所述，基于 Gabor 滤波的增强算法是顺着脊线的方向使用 Gabor 窗函数去过滤图像，那么首先需要知道局部脊线的方向，这些局部脊线方向就构成了方向图。方向图描述了指纹图像中每一像素点所在脊线或谷线在该点的切线方向，作为一种可直接从原灰度图像中得到的有用信息，它的计算一直是指纹识别技术中必不可少的一步。方向图也可看作是指纹图像的一种变换表示方法，即用脊线的方向来表示该脊线。方向图分为两种：一种是点方向图，表示指纹图像中每一点脊线的方向；另一种是块方向图，表示指纹图像中每一块脊线的大致方向。

计算方向图的基本思想是，在指纹归一化图像上计算每一点（或每一块）在各个方向上的某个统计量（如灰度差、梯度等），根据这些统计量在各个方向上的差异，确定该点（该块）的方向。在实际处理中，往往用到块方向图，因为块方向图往往比点方向图有着更强的抗噪性，而且，块方向图可以减少计算量，有利于模块化的处理。块方向图可以由点方向图得到，也可以用最小均方估计算法求得。而基于 Gabor 滤波的增强算法中就使用了块方向图，算法的主要步骤如下：

(1) 将归一化图像 G 分为 $W\times W$ 大小的块（16×16）；

(2) 计算每一像素点 (i,j) 的梯度 $\partial_x(i,j)$ 和 $\partial_y(i,j)$。基于计算要求，梯度算子可以是 sobel 算子，也可以是更为复杂的 Warr-Hildreth 算子。例如 3×3 大小的 Sobel 算子如下：

$$\mathbf{Sobel}_x=\begin{bmatrix}-1 & 0 & 1\\ -2 & 0 & 2\\ -1 & 0 & 1\end{bmatrix}\qquad \mathbf{Sobel}_y=\begin{bmatrix}-1 & -2 & 1\\ 0 & 0 & 0\\ 1 & 2 & 1\end{bmatrix}$$

(3) 以像素点 (i,j) 为中心，用下面的公式估算每一块的方向场。

$$\gamma_x(i,j)=\sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}}\sum_{v=i-\frac{w}{2}}^{j+\frac{w}{2}}2\partial_x(u,v)\partial_y(u,v) \tag{8-2}$$

$$\gamma_y(i,j)=\sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}}\sum_{v=i-\frac{w}{2}}^{j+\frac{w}{2}}\left[\partial_x^2(u,v)-\partial_y^2(u,v)\right] \tag{8-3}$$

$$\theta(i,j)=\frac{1}{2}\arctan\left(\frac{\gamma_y(i,j)}{\gamma_x(i,j)}\right) \tag{8-4}$$

$\theta(i,j)$是在以像素(i,j)为中心的块上用最小平方估计局部脊线的方向场。从数学上讲,它代表了与 $W\times W$ 窗内傅里叶谱主方向垂直的方向。因为输入图像中有噪音,以及被毁坏的脊线谷线和细节点,估算的局部方向场 $\theta(i,j)$并不一定总是正确的。由于局部方向场在没有奇异点出现的局部邻域上有缓慢变化,可以用低通滤波器来修正不准确的局部脊线方向。为了实现低通滤波,方向图需要被转化为连续矢量场,其定义如下:

$$\Phi_x(i,j)=\cos(2\theta(i,j)) \tag{8-5}$$

$$\Phi_y(i,j)=\sin(2\theta(i,j)) \tag{8-6}$$

在这里 Φ_x和Φ_y分别是矢量场的 x 轴和 y 轴分量。对得到的向量进行低通滤波,如式(8-7)、式(8-8)所示。

$$\Phi'_x(i,j)=\sum_{U=-W\Phi/2}^{W_\phi/2}\sum_{V=-W\Phi/2}^{W_\phi/2}W(u,v)\Phi_x(i-u w,j-v w) \tag{8-7}$$

$$\Phi'_y(i,j)=\sum_{U=-W\Phi/2}^{W_\phi/2}\sum_{V=-W\Phi/2}^{W_\phi/2}W(u,v)\Phi_y(i-u w,j-v w) \tag{8-8}$$

这里,W 是一个的二维低通滤波,其中 $W_\phi\times W_\phi$定义了滤波器的大小,注意平滑操作是在块上进行的,滤波器大小的默认值是 5×5。

(4) 用以下公式来计算(i,j)处的局部脊线方向 $O(i,j)$。

$$O(i,j)=\frac{1}{2}\arctan\left(\frac{\Phi'_x(i,j)}{\Phi'_y(i,j)}\right) \tag{8-9}$$

用这个算法可以获得一个相当平滑的方向场。指纹的方向图,如图 8-3 所示。从图 8-3(b)我们可以看到方向图描述了脊线的大致走向。

(a) 指纹原图像　　(b) 指纹方向图像

图 8-3　指纹方向图

伪代码如下:

for each non-overlapping block $B(x,y)$ in the $N(x,y)$
    Compute the gradient of each pixel in $B(x,y)$;
    The mean of the gradient of all pixels in $B(x,y)$ acts as the gradient of $B(x,y)$;
    Compute the Orientation of $B(x,y)$;
    Smoothen orientation map $O(x,y)$by low-pass filter to yild $O'(x,y)$;

8.2.3 频率图

基于 Gabor 滤波的增强算法所用到的 Gabor 滤波器有多个参数,其中一个重要的参数就是局部脊线的频率,这些局部脊线的频率则构成了指纹图像频率图。通常,脊线频率的计算有两种方法:谱分析法和统计窗法。谱分析法是利用指纹图像频域上的特征进行估计,估计精度不是很高,但对噪声不敏感。统计窗法是在一定方向上统计指纹图像的灰度值,根据统计得到的峰值与谷值,进行脊线距离估计,该方法精度较谱分析要高一些,但对噪声敏感。因此,谱分析法适合背景噪声大、图像模糊的低质量图像;统计窗法适合背景噪声小、图像清晰的高质量图像。

在这里,我们使用一种经典的统计窗法来估计指纹图像中某一块的频率。当然,频率图像是在归一化图像 G 和方向图像 O 基础上获得。算法如下:

(1) 对于每一个方向图中的块(大小为 16×16),以块中心为原点建立脊坐标系(即 x 轴垂直于脊方向,y 轴平行于脊方向),在此坐标系内建立方向窗口,如图 8-4 所示。

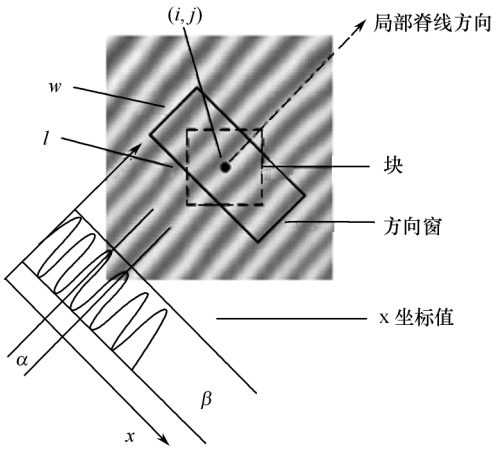


图 8-4　用于计算频率的方向窗

(2) 对每一块计算 x 的坐标值(x-signature),计算公式如下:

$$X[k]=\frac{1}{w}\sum_{d=0}^{w-1}G(u,v),\quad k=0,1,\cdots,l-1 \tag{8-10}$$

$$u=i+\left(d-\frac{w}{2}\right)\cos O(i,j)+\left(k-\frac{l}{2}\right)\sin O(i,j) \tag{8-11}$$

$$v=j+\left(d-\frac{w}{2}\right)\sin O(i,j)+\left(\frac{l}{2}-k\right)\cos O(i,j) \tag{8-12}$$

u 和 v 分别表示在图 8-4 中方向窗坐标系的横坐标表值与纵坐标值；$X[k]$表示了方向窗中横坐标上所有像素点的平均灰度值，我们记为 x 的坐标值。

如果没有细节点和奇异点出现在方向窗口内，x 的坐标值可以建立一个离散的正弦波形，若 $T(i,j)$为此正弦波两个相邻波峰间的平均像素点数的话，则该方向窗口的频率为：$\Omega(i,j)=1/T(i,j)$，假设窗口内没有连续的波峰，则将频率设为-1，以此区别于可用频率。

(3) 对于具有固定分辨率的扫描图像，脊线频率在一定范围内浮动。对于分辨率为 500dpi 的图像，这个范围为$[1/25,1/3]$，所以一旦超过这个范围，将频率设为-1。

(4) 对于存在细节点和奇异点的块，我们可以依据相邻块的频率，计算一个插入值，插入值计算方法如下：

$$\Omega'(i,j)=\begin{cases}\Omega(i,j) & \text{如果 } \Omega(i,j)\neq -1\\ \dfrac{\sum_{u=-w_\Omega/2}^{w_\Omega/2}\sum_{v=-w_\Omega/2}^{w_\Omega/2}W_g(u,v)\mu(\Omega(i-uw,j-vw))}{\sum_{u=-w_\Omega/2}^{w_\Omega/2}\sum_{v=-w_\Omega/2}^{w_\Omega/2}W_g(u,v)\delta(\Omega(i-uw,j-vw)+1)} & \text{其它}\end{cases} \tag{8-13}$$

$$\mu(x)=\begin{cases}0 & \text{如果 } x\leqslant 0\\ x & \text{其它}\end{cases}$$

$$\delta(x)=\begin{cases}0 & \text{如果 } x\leqslant 0\\ 1 & \text{其它}\end{cases}$$

W_g为一个高斯核函数，大小 $w_\Omega=7$。

(5) 使用低通滤波器对频率进行去噪处理。

$$F(i,j)=\sum_{u=-w_\Omega/2}^{w_1/2}\sum_{v=-w_\Omega/2}^{w_1/2}W_l(u,v)\Omega'(i-uw,i-vw) \tag{8-14}$$

W_l是一个二维低通滤波器，滤波器大小 $w_l=7$。

伪代码如下：

```
for each non-overlapping block B(x,y) in the N(x,y)
    Establish the Oriented Window
    Compute the x-signatures of the Oriented Window;
    Seek the peaks of x-signatures in the Oriented Window, the numbers of pixels
    between two adjacentpeaks is T, 1/T is the frequency of the Oriented Window,
    Smoothen frequency map F(x,y) by low-pass filter to yield F'(x,y);
```

8.2.4　区域 Mask

当上述方向场和频率场都已得出时，下一步就是对指纹图像进行滤波，但是有些指纹

图像质量太低的话，增强的效果并不是太好，因此对这样的指纹图像进行滤波就是多余的，我们应该摒弃这些指纹图像，重新录入，以获得质量更好的指纹图像。区域 Mask 就是一种判断指纹图像质量好坏的方法，它描述了输入图像中的每个像素可能属于可恢复区域，或者属于不可恢复区域。不可恢复区域过大时就该舍弃这些指纹图像。

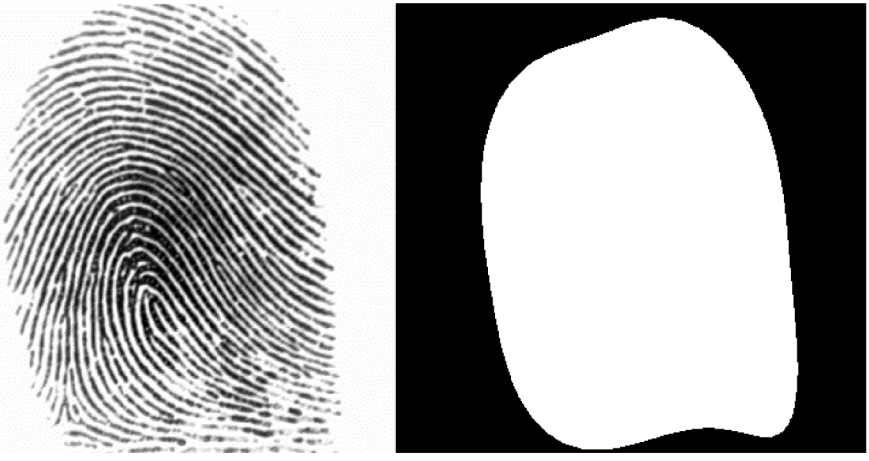
在本算法中，用三个特征来表征正弦曲线波形，分别为振幅(Amplitude)α，频率(Frequency)β和方差γ。设 $X[1],X[2],\cdots,X[I]$是以(i,j)为中心块的 x 的坐标值。上述三个特征可以用以下步骤来计算：

(1) α 为峰值的平均高度减去波谷的平均深度。

(2) $\beta=\dfrac{1}{T(i,j)}$，其中 $T(i,j)$是两个连续峰值点之间的像素点个数。

(3) $$\gamma=\frac{1}{I}\sum_{i=1}^{I}\left[X[i]-\left(\frac{1}{I}\sum_{i=1}^{I}X[i]\right)\right]^2 \tag{8-15}$$

对于每个像素点，上述三个特征构成一个三维向量，然后使用方差聚类算法将其划分为 6 类，前 4 类划分到可恢复区域，后 2 类划分到不可恢复区域。接着将指纹图像分割为不重合的、大小为 $W\times W$ 的像素块。如果像素点(i,j)划分至可恢复区域，则一个以(i,j)为中心的块为可恢复区域，那么块 $R(i,j)=1$，否则，$R(i,j)=0$。得到图像 R 后，可恢复区域所占的比例就能计算出来。一个被接受的图像才能进入到下一步的滤波中。如果可恢复区域的比例比阈值小，那么这个输入指纹图像就会被拒绝。得到的区域 Mask，如图 8-5所示，在图(b)中，白色的区域为有效区域，黑色的区域为无效区域。



(a) 指纹原图像　　(b) 指纹区域 Mask 图像

图 8-5　区域 Mask 图像

8.2.5　滤波

获得了脊线的方向和频率，就可以对指纹块图像进行滤波。滤波有空域和频域两种滤波方法。一般来讲，空域滤波法适合高质量的指纹图像，频域滤波法适合低质量的指纹

图像。由于指纹图像的非均匀性，将单一参数的滤波器应用于整个图像是不切合实际的，相反，为加强脊线结构的显现，滤波器的参数应具有自适应性。因此，大多数现有的技术是基于局部脊线频率和方向的纹理滤波器。

在平行于局部区域脊线的基础上，我们定义了指纹图像的频率和方向，这些信息将能很好地消除噪声，并且在这个局部区域内，指纹图像具有恒定的方向和变化缓慢的频率。所以，具有相应方向和频率的带通滤波器可以有效地去噪，使脊线结构更加明朗。

Gabor 滤波器具有频率选择性和方向选择性，因此可以调节 Gabor 滤波器的方向系数和频率系数，使其在平行于指纹脊线方向上进行带通滤波。由 Gabor 滤波器的数学模型可以看出，此种滤波器在 x 方向上为带通，y 方向上为低通。在对指纹图像进行滤波时，只需对滤波器进行旋转，使其与指纹方向场一致，就可以实现对指纹脊线信息最大限度地增强，而垂直于指纹方向场的信息则相对减弱。

偶对称 Gabor 滤波器的表达式如式(8-16)、式(8-17)和式(8-18)所示。Gabor 滤波器的空域表达如图 8-6 所示，其频域表达如图 8-7 所示。

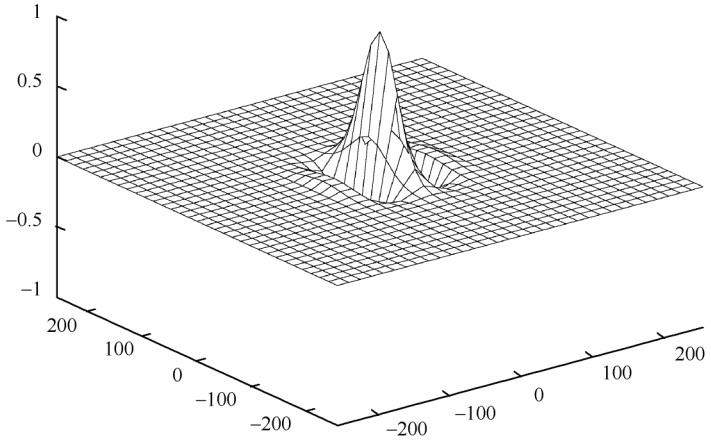


图 8-6　实对称 Gabor 滤波器

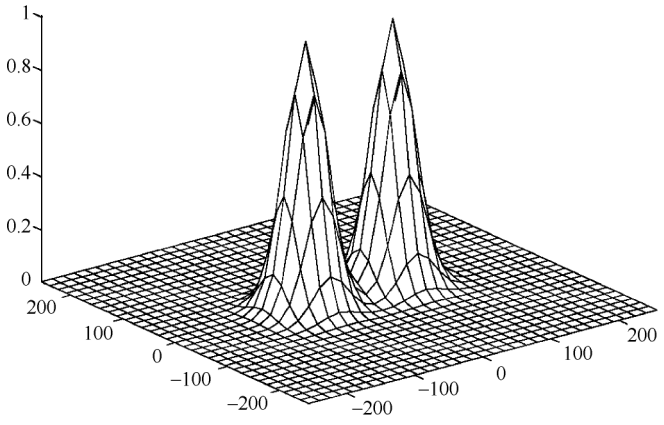


图 8-7　相应的传递函数

$$h(x,y;\phi,f)=\exp\left\{-\frac{1}{2}\left[\frac{x_\phi^2}{\delta_x^2}+\frac{y_\phi^2}{\delta_y^2}\right]\right\}\cos(2\pi f x_\phi) \tag{8-16}$$

$$x_\phi=x\cos\phi+y\sin\phi \tag{8-17}$$

$$y_\phi=-x\sin\phi+y\cos\phi \tag{8-18}$$

式中，ϕ 是滤波器的方向，这里即是脊线的方向；f 是滤波器的频率，这里即为方向窗口内的频率；δ_x、δ_y 分别是高斯包络沿 x 轴和 y 轴的标准差在这里均取 4.0，它们都是通过实验所得的经验值。

将方向和频率值分别带入 ϕ 和 f，再将此滤波器与相应块内的指纹图像进行卷积，便可得到增强后的图像 $E(i,j)$（也可在傅里叶域进行处理）。计算如式(8-19)所示。

$$E(i,j)=\sum_{u=-w_g/2}^{w_g/2}\sum_{v=-w_g/2}^{w_g/2}h(u,v,O(i,j),F(i,j))G(i-u,j-v) \tag{8-19}$$

通过滤波后，我们得到的最终增强后的指纹图像如图 8-8 所示，与原始指纹图像比较，我们可以看到，增强后的指纹图像，脊线结构更加清晰且连续，但又不失重要的特征信息。

(a) 指纹原图像　　(b) 增强后的指纹图像

图 8-8　增强效果对比

伪代码如下：

```
for each non-overlapping block B(x,y) in the N(x,y)
    O'(x,y) and F'(x,y)acts as angel parameter and frequency parameter of the Gabor filter,
do_gabor_filtering(N(x,y),O'(x,y),O'(x,y));
```

8.3　基于方向各向异性滤波的增强算法

基于方向各向异性滤波的增强算法与前面所述的基于 Gabor 滤波的增强算法有相同的地方，也有不同之处。相同之处在于增强图像之前，我们仍需对原指纹图像进行归一化和求取方向图；不同之处在于该算法利用方向图构造了各向异性滤波器，再使用该滤波

器对归一化后的图像进行滤波，这个滤波器的主轴平行于局部脊线方向，所以这个滤波器可以沿着脊线方向对图像像素进行平滑，从而达到图像增强的效果。

各向异性的滤波器可以用公式(8-20)来表示：

$$H(x_0,x)=V+S_p(x-x_0)\exp\left\{-\left[\frac{(x-x_0\cdot n_\perp)^2}{\sigma_1^2(x_0)}+\frac{(x-x_0\cdot n_\perp)^2}{\sigma_2^2(x_0)}\right]\right\} \tag{8-20}$$

式中 $\boldsymbol{n}$ 和 $\boldsymbol{n}_\perp$ 是互相垂直的单位矢量，并且 $\boldsymbol{n}$ 平行于脊线方向，脊线方向可以从上一小节中提取到的指纹方向场中获得。S 和 V 控制了相位强度和外围像素。$\sigma_1^2(x_0)$ 和 $\sigma_2^2(x_0)$ 决定了高斯核的形状，它们是由 x_0 周围的频率信息估算出来的。只要 $\sigma_2^2(x_0)$ 的大小在平均脊线宽度附近，滤波器就不会对它们的值敏感。

应用上述方法对原指纹图像进行增强，得到的结果如图 8-9 所示。从图中可以看出，应用上述方法对指纹图像进行增强处理有很好的效果。

(a) 指纹原图像　　(b) 增强后的指纹图像

图 8-9　利用各向异性滤波增强效果对比

8.4　二值化

指纹图像增强之后，为了获取指纹特征，需要对增强后的图像进行二值化。二值图，即是将灰度图像用 1 或 0 进行二值表达。这样既对图像信息进行了压缩，减少了数据量，节约了存储空间，便于计算机存储和处理，同时又保留住了指纹图像中最重要的信息。除此之外，指纹图像二值化处理还去除了指纹错误连接，为指纹特征的提取和匹配做好准备。图像二值化的方法有固定阈值法和自适应阈值法。在这里我们介绍一种自适应阈值法：基于最大熵的二值化方法。

对于离散型随机变量 X 而言，假设有 N 种可能发生情况，分别记做 $a_i(i=1,2,\cdots,n)$，任意一种情况发生的概率为 p_i，信息熵 $H(X)$ 的计算方法如式(8-21)所示。

$$H(X)=\sum_{i=1}^{n}p_i\times\log(1/p_i) \tag{8-21}$$

信息熵之所以能用于指纹图像二值化，是因为熵代表图像中的指纹灰度信息量。当其概率相等时，信息熵的取值最大。最大信息熵法的目的就是使得系统稳定，在概率上实

现无偏分配。指纹图像中脊线和谷线交替出现，寻找到脊线和谷线交替处的像素点的灰度值将可以被我们用于指纹图像的二值化，因此只要找到的是使得信息熵最大的灰度值即可作为指纹图像二值化的阈值。

对于一副 256 阶的灰度指纹图像，灰度的变化范围为 0～255，求取最大信息熵 $H_t(t=1,2,\cdots,255)$来求取阈值 t，图像二值化的具体算法如下：

(1) 将指纹图像分为 $w\times w$ 的若干小块。

(2) 计算各个小块中每一个灰度阶 i 的概率，计算公式如下：

$$p_i=\frac{N_i}{w\times w} \tag{8-22}$$

式中，p_i为灰度阶 i 在小块中所占的概率；N_i为灰度阶 i 在小块中存在的总量；$w\times w$ 为块的大小。

(3) 假设一个灰度阶 t 可以把一个块分为脊线和谷线，则与灰度 t 对应的信息熵 H_t 的计算公式如下：

$$H_t=HB_t+HF_t \tag{8-23}$$

式中，HB_t为背景区域的信息熵；HF_t为脊线区域的信息熵。

HF_t的计算公式为：

$$HF_t=\sum_{i=1}^{n}\frac{p_i}{p_t}\log\left(\frac{p_i}{p_t}\right) \tag{8-24}$$

HB_t的计算公式为：

$$HB_t=\sum_{i=1}^{n}\frac{p_i}{1-p_t}\log\left(\frac{p_i}{1-p_t}\right) \tag{8-25}$$

式中，p_i 为灰度阶 i 的概率；$p_t=\sum_{i=0}^{t}p_i$ 为纹线区域对应的灰度阶的概率之和。

(4) 对每一个块利用式(8-23)计算出其对应的最大熵 H_t，将对应的灰度阶 t 作为指纹图像二值化的阈值，并利用该阈值对该块进行二值化处理，处理方法如式(8-26)所示：

$$G(x,y)=\begin{cases}255, G(x,y)\geqslant T\\ 0, G(x,y)<T\end{cases} \tag{8-26}$$

式中 $G(x,y)$代表块中像素点的灰度值。

通过以上操作，我们即可得到二值化后的图像，如图 8-10 所示。从图 8-10(b)中，我们看到二值化后的图像纹理更加清晰，脊线与谷线的对比度明显，利于提取细节特征。

伪代码如下：

```
for each non-overlapping block B(x,y)
    for t=1:256
        initialize the variable m=0;
        calculate the entropy;
        m:=max(entropy);
        t=t+1;
    end
        save m;
use m as the threshold, binarize the block B(x,y)
```

(a) 指纹原图像　　(b) 二值化指纹图像

图 8-10　二值化效果对比

8.5　本章小结

本章简单介绍了多种指纹图像的增强算法，并着重介绍其中一种较为经典的 Gabor 滤波增强算法。与此对比，又简单地介绍了基于方向各向异性滤波器的增强算法。然后对两种算法都进行了详细的步骤分解，并对每一步骤进行数学阐述。在最后还讲述了增强的后续操作——二值化，它的目的是为特征提取做准备，二值化图像也可减少信息量的存储，加快特征提取的时效。

习题与思考题

1. 指纹图像增强的目的是什么？
2. 基于 Gabor 滤波增强算法的步骤包括哪些？
3. 从图 8-8(b)中增强后的指纹图像来看，基于 Gabor 滤波增强的方法有哪些不足的地方？
4. 对图像归一化的目的是什么，归一化对增强的后续步骤有什么帮助？
5. 什么是指纹的方向图、频率图？
6. 基于 Gabor 滤波增强的方法中，频率图是如何通过方向图得到的？
7. 滤波分为哪些滤波方法，各个滤波方法是怎样滤波的？
8. 滤波的目的是什么，滤波后的图像与原图像会有什么不同？
9. 什么是二值化，为何要对图像进行二值化？

第 9 章　指纹图像特征提取与匹配

指纹图像特征提取是从指纹图像中获取可以代表该指纹图像的特征信息的过程。指纹图像匹配是比对从两幅指纹图像中提取出的特征信息，判断这两幅指纹是否来自于同一手指所采集的指纹的过程。

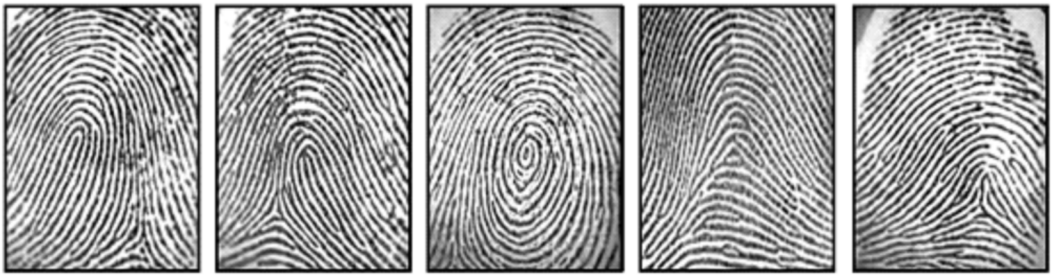
指纹图像特征提取与匹配是自动指纹识别中最重要的两个步骤，其算法的好坏直接影响自动指纹识别系统的识别结果。

本章主要介绍指纹图像特征提取与匹配，其中 9.1 节介绍常用的指纹特征提取与匹配算法，9.2 节介绍应用链码对指纹进行特征提取的算法，9.3 节介绍应用方向描述子进行指纹特征匹配的算法，9.4 节对本章做出总结。

9.1　经典的指纹特征提取与匹配算法

指纹图像的特征点被分为两大类，一类是全局特征点，另一类是局部特征点。全局特征又分为指纹类型特征和奇异点特征。

指纹类型特征用于指纹的分类，它指的是指纹中脊线的总体走向。根据指纹类型特征可以将指纹分成 5 类：左旋、右旋、螺旋、拱和尖拱，如图 9-1 所示。



(a) 左旋指纹　(b) 右旋指纹　(c) 螺旋指纹　(d) 拱型指纹　(e) 尖拱指纹

图 9-1　5 种基本的纹线类型

奇异点特征又可分为三角点和中心点，如图 9-2 所示。三角点和中心点常用于指纹图像的配准。

局部特征是指指纹图像中的细节特征。指纹细节特征有多种类型，如终结点、分叉点、湖、独立脊线、点或岛、毛刺和桥等，如图 9-3 所示。

指纹图像的细节特征中，终结点和分叉点常用来做指纹图像匹配。下面将介绍这两类指纹细节点传统的提取算法和匹配算法。

图 9-2　指纹的中心点和三角点

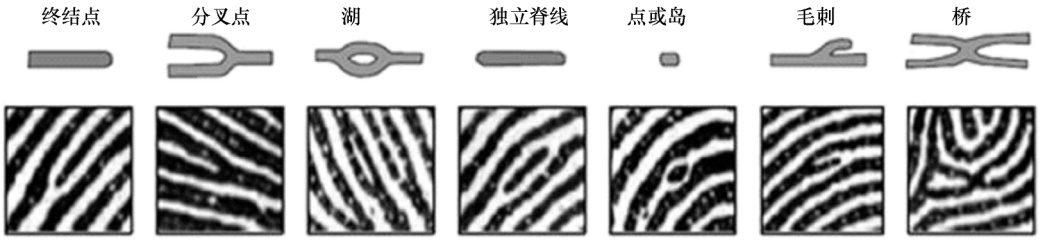


图 9-3　7 种常见的细节点类型

9.1.1　经典的指纹细节点提取算法

指纹图像的终结点和分叉点的提取方法有很多，下面将详细介绍利用 8 邻域模版提取指纹特征点的方法。

在提取指纹图像的分叉点和终结点之前，首先分析一下终结点和分叉点的 8 邻域内像素的特征。

在细化后的指纹图像中建立模版，假设终结点和分叉点如图 9-4 所示，那么终结点周围 8 个像素只有一个值为 1，其余的为 0，因此，终结点周围像素的值顺序变化（从 0 到 1，或从 1 到 0）的次数为 2；分叉点周围像素的值顺序变化（从 0 到 1，或从 1 到 0）的次数为 6；而脊线的连续点周围 8 个像素有两个值为 1，其余为 0，因此连续点周围像素顺序变化（从 0 到 1，或从 1 到 0）的次数为 4，所以可以根据这些细节特征信息来判断特征点的存在。

根据上述特点，在细化后的指纹图像中建立 3×3 的模版（图 9-4 所示），求交叉数 CN（Crossing Number）就可以来判断细节特征。判断方法的公式为

$$\mathrm{CN} = \sum_{i=0}^{7} |P_i - P_{i+1}| \tag{9-1}$$

0	0	0
0	P	1
0	0	0

(a)P 为终结点

0	1	0
0	P	1
1	0	0

(b)P 为分叉点

图 9-4　细节特征 8 邻域

式中，P_i表示像素 P 周围的 8 个像素的灰度值，$P_i=0$ 或 $P_i=1$。

图 9-5 是从细化后的指纹图中截取的一小部分，从图中可以看出，如果 CN=2，则模板中心为指纹脊线终结点；CN=6，则为分叉点；CN=4，则为连续脊线。扫描完整幅图像后，可得其全部的特征点。

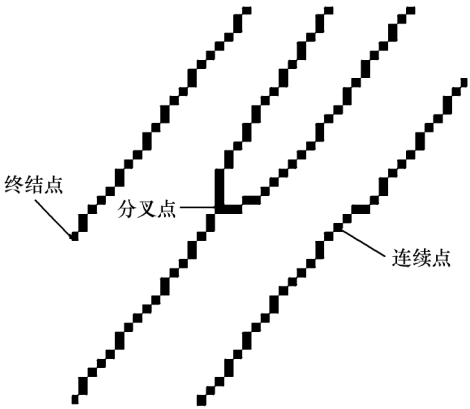


图 9-5　细化的指纹图像

然而这种传统的指纹细节点提取算法是基于细化的指纹图像，而指纹图像的细化算法耗时较长，从而影响指纹识别系统的整体性能。

另一种指纹细节点提取算法是在二值化的指纹图像上直接进行指纹特征提取，提取过程中并不需要进行细化操作，因此大大节省了图像处理时间，提取出的特征信息也是准确可靠的。

在 9.2 节将详细介绍应用链码进行特征提取的算法，该算法便是在二值化的指纹图像上进行特征提取的。

9.1.2　经典的指纹细节点匹配算法

指纹图像的匹配算法是通过比对从两幅指纹图像中提取到的特征信息来进行匹配的。指纹图像匹配是指纹识别的最后一个环节，通过指纹图像的匹配得到指纹图像最终的识别结果，所以指纹图像匹配也是指纹识别中最为关键的环节。

目前已有多种指纹匹配算法提出，包括基于图匹配的方法、基于纹理特征匹配的方法和基于细节点模式的匹配方法等。目前为止，使用最多的还是基于细节点模式的匹配方法。

在理想情况下，如果输入的细节点和模板细节点之间不存在平移、旋转和尺度变形，并且指纹图像中的每个细节点都被准确地提取出来，且没有虚假细节点，那么细节点匹配仅需统计重合细节点的对数，如果超过一定数目，即可判定为匹配。

然而在实际应用中，受各种主客观因素的影响，以上条件很难完全满足。首先，由于在采集指纹时无法对手指与采集设备表面的接触方向、位置、按压用力方向和手指按压力度等做出严格的限制，从而不仅会使相同手指在不同时间所采集到图像区域不完全相同，而且图像之间不可避免地存在平移变形、旋转变形、尺度变形和非线性变形。

其次，当图像质量较差时，细节点提取过程会产生很多误差，包括产生虚假细节点、遗漏真实细节点，以及细节点位置、方向偏差。这些因素造成即使是相同手指的指纹图像，其中细节点的数量、位置、方向等也不完全相同，使指纹细节点匹配问题变得非常困难。

基于以上问题可知，我们需要一种能对指纹图像平移、旋转有着很好的鲁棒性的匹配算法来进行指纹特征匹配。本章 9.3 介绍的应用方向场描述子(Tico)进行特征匹配的算法就很好地解决了由指纹图像的平移、旋转带来的匹配困难问题。

9.2　应用链码进行特征提取

链码是一种对黑白图像进行无损压缩的算法，链码的基本原理是将图像中连续的部分进行分别编码。对于图像中每个连续的部分，边界上的点的坐标和方向信息等都将被连续的保存下来。

利用链码来表示物体的轮廓已经得到了广泛的应用。与细化骨架不同，图像中每个像素都可以从链码中完全恢复到它本身的轮廓。在指纹图像中，利用链码可依次保存下每个连续部分的边界坐标，追踪链码就可以获得每条脊线的轮廓的坐标及方向信息。根据获得的脊线轮廓的信息，我们就可以提取到指纹的终结点和分叉点。

应用链码来提取指纹细节点分为以下几个步骤：指纹图像增强、指纹细节点特征提取和虚假细节点的删除。

在本书第 8 章介绍过一些常用的指纹图像增强算法，在应用链码进行指纹细节点特征提取时，我们使用 8.3 节的增强方法对图 9-6 中的(a)图进行增强，得到如图(b)所示的图像，对图(b)进行二值化得到图(c)。图(c)将用于下一节的指纹细节点特征提取。

(a)FVC2002 指纹库中的指纹图像　　(b)增强后的指纹图像　　(c)二值化后的指纹图像

图 9-6　指纹图像增强和二值化图

9.2.1 指纹细节点特征提取

对上一节中得到的二值化的指纹图像通过以下几个步骤便可以提取到指纹细节点：

(1) 通过从上到下、从左到右扫描一幅指纹图像，获得指纹图像中脊线的轮廓。

(2) 逆时针方向追踪脊线的轮廓，并把脊线上的元素信息记录在一个数组里。

(3) 根据记录的信息来计算获取指纹图像的细节点。

每一个轮廓元素就是轮廓上的每一个像素点。它包括这个像素点的 x，y 坐标、轮廓上像素的斜率或者方向以及附加的信息(如曲率)等，如图 9-7 所示。

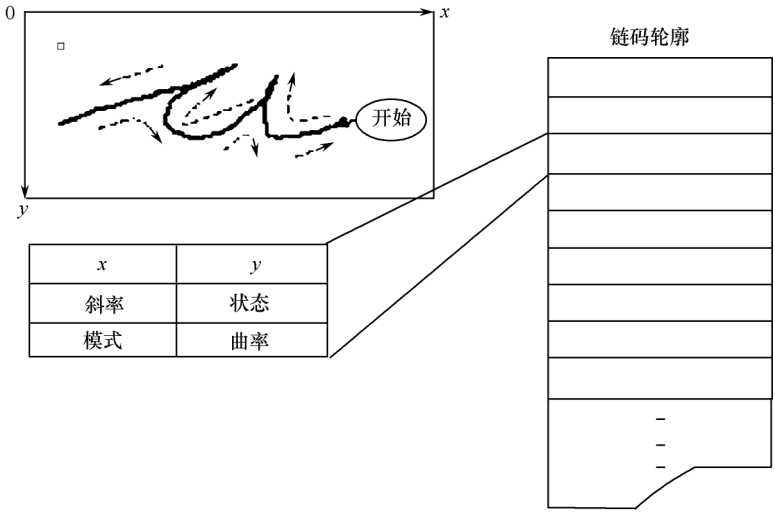


图 9-7　应用链码表示轮廓

在一个二值化的指纹图像中，脊线不止一个像素宽。沿着脊线的边界逆时针方向追踪脊线，当发生明显的左转时，这个点就被认为是终结点；同样的，当发生明显的右转的时候，这个点被认为是分叉点，如图 9-8 所示。

定义 p_{in} 为点 P 的入射向量，p_{out} 为该点的出射向量。通过 P 点周围的一些临近的轮廓上的点，可以计算出 p_{in} 和 p_{out}。这样可以避免一些局部噪声并且同时可以通过使用多个点的平均值获得较好的两个向量的估计值。

脊线轮廓上 P 点方向改变的大小 θ，由两个向量 p_{in} 和 p_{out} 之间的夹角大小决定，如式(9-2)所示：

$$\theta=\arccos\frac{p_{in}\cdot p_{out}}{|p_{in}||p_{out}|} \tag{9-2}$$

式中 $p_{in}\cdot p_{out}$ 表示这两个向量的点积；$|p_{in}||p_{out}|$ 表示两个向量模的乘积，arccos 表示反余弦函数。

在大小归一化之后，让两个向量分别为 $p_{in}=(x_1,y_1)$，$p_{out}=(x_2,y_2)$，那么 θ 的大小可由式(9-3)确定：

$$\theta=\arccos(x_1x_2+y_1y_2) \tag{9-3}$$

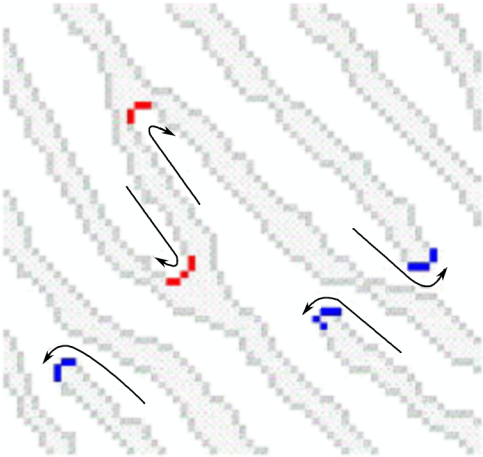


图 9-8　指纹细节点图

定义一个阈值 T 使得所有显著的转向都符合式(9-5)的情况，并且所有符合式(9-4)的条件的点都被认为是细节点：

$$x_1x_2+y_1y_2<T \tag{9-4}$$

如过我们把这两个向量放在笛卡儿坐标系中，p_{in} 沿着 x 轴，那么阈值 T 就是一个垂直于 x 轴的线，如图 9-9 所示。因为角度 θ 总是在 $-90°\sim90°$ 之间，所以两个向量的旋转方向可由 $\sin\theta$ 表示，如式(9-5)所示：

$$\sin\theta=x_1y_2-x_2y_1 \tag{9-5}$$

其中 $x_1y_2-x_2y_1>0$ 表示左转；$x_1y_2-x_2y_1<0$ 表示右转；$x_1y_2-x_2y_1=0$ 表示没有转弯。

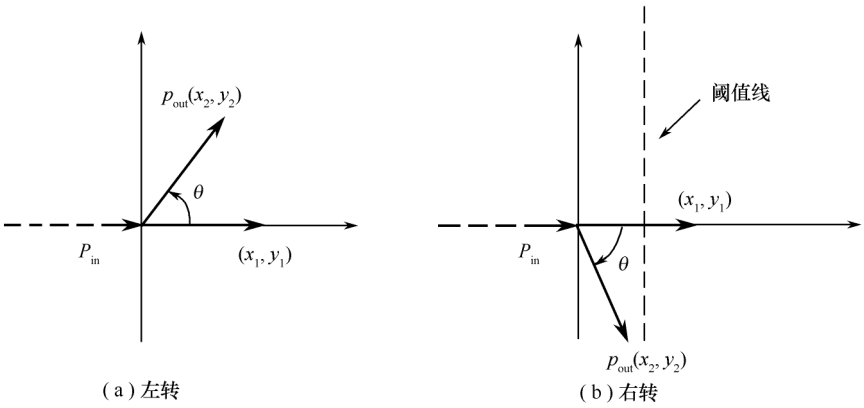


图 9-9　入射出射向量示意图

经过以上步骤，应用链码方法对图 9-6 中的(c)图进行细节点提取获得的指纹细节点如图 9-10 所示。从图中可以看出，前景区域的细节点绝大部分都被提取出来了，只有个别的细节点被漏掉了。总体来说，应用链码进行指纹细节点特征提取的效果是不错的。

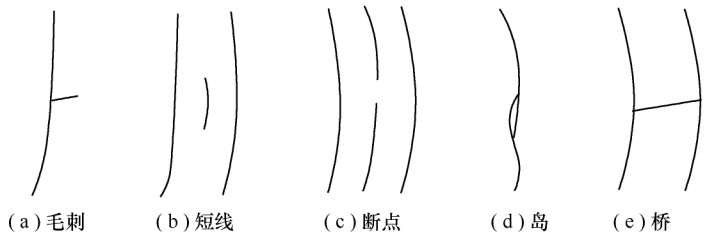
(a) 指纹原图　　(b) 细节点图

图 9-10　应用链码获得细节点图

9.2.2　虚假细节点的删除

通过指纹细节点提取获得的指纹细节点绝大部分是真实的，但其中不可避免地包括由于噪声产生的虚假细节点。虚假细节点的存在会严重影响指纹匹配的结果，所以在进行指纹匹配之前需要去除虚假细节点。

在对指纹进行预处理后，图像中存在着大量的毛刺、短线、断点、岛和桥等噪声，如图 9-11 所示。我们从中提取到的细节特征，往往包含大量的伪特征信息。但如果深入分析指纹图像中各类噪声的特点，总结出虚假细节点的形成原因和分布规律，就可以设计相应的算法，去伪存真，筛选出真正的细节点集。



(a) 毛刺　(b) 短线　(c) 断点　(d) 岛　(e) 桥

图 9-11　指纹图中存在的噪声

未经修复处理的指纹图像中，主要存在以下几类噪声。

(1) 毛刺

毛刺是由随机噪声导致二值图中脊线不光滑而形成的。这种位置可以检测到一个脊线终结点和一个脊线分叉点，属于虚假细节点。这种虚假细节点的特点是一对终结点与分叉点之间有脊线相连，且两点之间距离比较小。

(2) 短线

当手指表面不干净时，采集到的指纹图像容易出现较多的短线，短线的出现主要是由

随机噪声引起的。在这种位置，会提取到两个脊线终结点，属于虚假细节点。这种虚假细节点的特点是两点之间距离很小，两点之间由一条脊线相连。

(3) 断点

当指头比较干或者采集指纹时手指用力不均时，采集到的指纹图像往往存在大量的脊线断点。在脊线有断点的地方，细节特征提取算法就会检测到两个脊线终结点，属于虚假细节点。这种虚假细节点的特点是两点之间距离很小且两点之间的区域没有脊线存在。

(4) 岛

岛的出现主要是由于随机噪声的影响而形成的。在这种位置可以检测到两个分叉点，属于虚假细节点。这种虚假细节点的特点是两点之间的距离非常小，且两点之间连线与其局部邻域脊线的方向近似平行。

(5) 桥

当手指比较湿或者比较脏或者采集指纹用力不均时，采集到的指纹图像往往会出现较多相邻脊线连在一起的现象，即本不应该相连的脊线粘连在一起。在这种位置，细节特征提取算法会提取到两个脊线分叉点，属于虚假细节点。这种虚假细节点的特点是两点均为脊线分叉点，两点之间的距离恰好近似等于平均脊线间距，而且两点之间连线近似垂直于其局部邻域的脊线方向。

由于上述噪声的存在，就会使提取到的特征中存在伪特征信息。根据上述伪特征的特点，选择合适的伪特征去除算法对每一种伪特征进行有针对的去除。

定义 $D(i,j)$为两细节点 i、j 之间的距离，单位为像素；$A(i,j)$为两细节点 i、j 之间的夹角的绝对值，单位为弧度；如果两个细节点 i、j 之间是连续的，则定义 $C(i,j)=1$；否则，$C(i,j)=0$。

(1) 毛刺形成的虚假细节点的删除

原始细节点集中，对于任意一个终结点 i 和一个分叉点 j，如果 $D(i,j)<D_1$ 并且 $C(i,j)=1$，则判断该终结点为虚假细节点并删除。

(2) 短线形成的虚假细节点的删除

原始细节点集中，对任意两个终结点 i、j，如果 $D(i,j)<D_2$，$A(i,j)=\pi$ 并且 $C(i,j)=1$，则判断该两点为虚假细节点并删除。

(3) 断点形成的虚假细节点的删除

原始细节点集中，对任意两个终结点 i、j，如果 $D(i,j)<D_3$，$A(i,j)=\pi$ 并且 $C(i,j)=0$，则判断该两点为虚假细节点并删除。

(4) 岛形成的虚假细节点的删除

原始细节点集中，对任意两个分叉点 i、j，如果 $D(i,j)<D_4$，$A(i,j)=\pi$ 且 $C(i,j)=1$，则判断该两点为虚假细节点并删除。

(5) 桥形成的虚假细节点的删除

原始细节点集中，对任意两个分叉点 i、j，如果 $D(i,j)=D_5$ 且 $C(i,j)=1$，则判断该两点为虚假细节点并删除。

其中，D_1、D_2、D_3、D_4 都为距离的阈值，D_5 为指纹平均脊线宽度，它们的大小都可根据

指纹图像的分辨率给出。

删除以上虚假细节点后，留下的细节点就是真正的、可靠的指纹细节点。这些真实可靠的细节点就可以用于下一节应用方向场描述子(Tico)对指纹进行特征匹配中。

应用链码进行特征提取的伪代码如下：

```
Procedure Minutiaes Extraction
        input:fingerprint image Img
        output:minutiaes M(M1、M2、M3,…)
        ImgBin←the binary image of Img
        Con(Con1,Con2,…)←the contour of ImgBin
        Num←the number of Con
        counter←1
        Min_Con←define the minimum size of Con
        Min_Cur←define the minimum curvature
        WHILE(counter<Num+1)
            Size_Con←the size of Con1,Con2,…
            IF(Size_Con<Min_Con)
                counter=counter+1
                CONTINUE
            ELSE
                (x,y)←the coordinates of each pixel point on the Con
                Cur←calculate the curvature of each pixel point
                Poi←the local maximum value point in Cur
                Poi_Cur←the curvature of Poi
                IF(Poi_Cur>Min_Cur)
                    Poi is a minutiae and save this point
                END IF
                counter=counter+1
            END IF
        END WHILE
    END Minutiaes Extraction
```

9.3 方向场描述子特征匹配

9.2 节已经应用链码算法获得了指纹的细节点信息，本节介绍应用方向描述子和细节点信息进行指纹匹配的方法。方向场描述子(Tico Descriptor)是 M. Tico 等人在 2003 年提出来的，他将细节点与方向场结合，构造了基于方向场的细节点描述子。Tico 描述子除了具有平移旋转不变性外，还具有描述子间相互独立的特征，可以用来计算相似度和指纹配准。下面将详细介绍 Tico 描述子的构造以及它用于指纹匹配的整体流程。

9.3.1　方向场描述子构造

由于方向场描述子需要使用到指纹细节点和方向场信息，因此，在构造方向场描述子前，首先要区分细节点的方向和指纹的方向场：细节点方向范围为$[0,2\pi)$，而指纹的方向场范围为$[0,\pi)$。

令α与β表示两个方向角，则α相对于β的角度定义为$\lambda(\alpha,\beta)$：即为β所在的直线沿逆时针旋转到与α所在直线平行的最小角度。为了表示两个方向的距离，用式(9-6)进行计算：

$$\Lambda(\alpha,\beta)=(2/\pi)\min(\lambda(\alpha,\beta),\lambda(\beta,\alpha)) \tag{9-6}$$

由式(9-6)可见，Λ的取值范围在0～1之间。当Λ取0时，表示两个方向平行，Λ取1时则表示两个方向垂直。

由于方向场具有局部一致性，因此，某区域内的方向场可以通过采样完全重构出来。以细节点为中心，在其邻域内进行方向场采样以表示这一区域的方向场特点。

Tico描述子的构造过程如下，以细节点为圆心，以r为半径作l个同心圆，每个圆上包含K_l个采样点$p_{k,l}$，其中l与k满足$1\leqslant l\leqslant L$与$1\leqslant k\leqslant K_L$。如图9-12所示，把细节点的方向作为初始方向，沿逆时针由内而外对采样点依次进行编号。令θ表示细节点的方向角度，$\theta_{k,l}$表示采样点$p_{k,l}$的方向角度，则基于方向场的细节点描述子可以由式(9-7)中的列向量表示：

$$f=\left\{\left[\lambda(\theta_{k,l},\theta)\right]_{k=1}^{K_l}\right\}_{l=1}^{L} \tag{9-7}$$

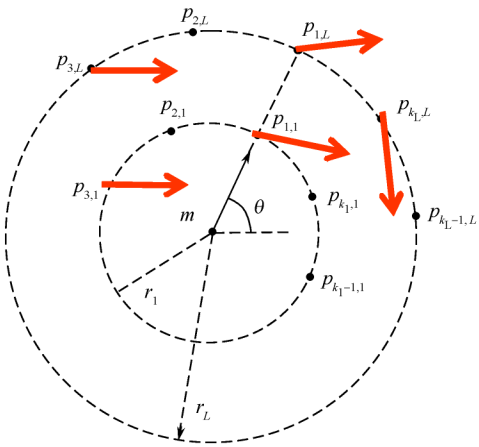


图 9-12　方向场描述子的拓扑结构，图中m为细节点，p为采样点，箭头为改点方向

根据上述构造过程可以得知Tico描述子具有平移与旋转不变性。所以即便指纹的方向与位置均发生改变，对应的细节点也可以由Tico描述子计算出很高的相似度，从而进行指纹配准与相似度计算。此外，Tico描述子还具有另外一个重要性质：描述子之间相互独立，这就在一定程度上缓解了因部分指纹区域发生形变而无法匹配的问题。

9.3.2 相似度计算

9.3.1 节我们使用细节点和周边的方向场信息构造了 Tico 描述子，下面对两个 Tico 描述子的相似度计算进行介绍。

假设 a、b 两个细节点对应的 Tico 描述子分别为 $f(a)=\{\alpha_{k,l}\}$ 与 $f(b)=\{\beta_{k,l}\}$，式(9-8)用于计算两个描述子的相似度：

$$S(a,b)=(1/K)\sum_{l=1}^{L}\sum_{k=1}^{K_l}s(x_{k,l}) \tag{9-8}$$

式中，$K=\sum_{l=1}^{L}K_l$；$x_{k,l}=\Lambda(\alpha_{k,l},\beta_{k,l})$；$s(x)=e^{(-16x)}$ 表示角度差为 x 的两个角度间的相似度，$s(0)=1$ 时表示两个角度之间相似度最大。

得到 Tico 描述子的相似度之后，就可以用相似度来确定两个细节点间的对应关系。

9.3.3 对应关系的确定

两个描述子间的相似度是确定其是否对应的重要线索。如果细节点 a_i 与 b_j 间的相似度较大，便可认为两个细节点对应。但如果出现如图 9-13 中的情况，因为指纹方向场的局部一致性，a_i 与 b_j 邻近的细节点也可能有较大的相似度。这就可能带来错误的细节点匹配。

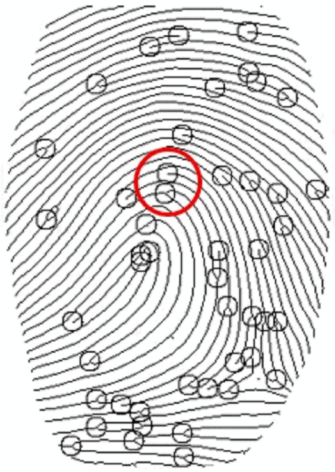


图 9-13　图中被圈出的两个细节点的 Tico 描述子会有很高的相似度

为了解决这个问题，需要满足以下两点才确定两个细节点是相似的：①a_i 与 b_j 相似度大；②a_i 与除 b_j 外的其它细节点相似度均小。为了量化这个过程，定义描述子之间的概率密度函数为：

$$P(a_i,b_j)=S(a_i,b_j)^2/\left[\sum_{i'=1}^{N}S(a_{i'},b_j)+\sum_{j'=1}^{M}S(a_i,b_{j'})-S(a_i,b_j)\right] \tag{9-9}$$

当且仅当 a_i 与 b_j 具有较高相似度时，上式获得最大值，再确定指纹细节点之间的对应关系，进而进行指纹的配准与匹配分数的计算。

9.3.4　配准与匹配分数的计算

匹配分数的计算与所有细节的相似度有关，在计算匹配分数之前，因为指纹的采集过程中每次获取的指纹图像不同，经常出现平移与旋转，所以需要利用相似度较高的细节点作为对准点对图像进行配准，然后计算整体的匹配分数。

通常选择具有高区分度的细节点作为对准点，计算出相应的的平移旋转参数，计算公式如下：

$$\begin{pmatrix}\Delta x\\ \Delta y\\ \Delta\theta\end{pmatrix}=\begin{pmatrix}x^d\\ y^d\\ \theta^d\end{pmatrix}-\begin{pmatrix}x^D\\ y^D\\ \theta^D\end{pmatrix} \tag{9-10}$$

其中，Δx、Δy、$\Delta\theta$ 为平移、旋转参数；上标 D 表示参考对准点；上标 d 则表示的是待配准对准点。获取旋转平移参数后，就可以进行坐标和角度变换。角度和坐标变换的计算方法如下：

$$\begin{pmatrix}x_i^A\\ y_i^A\\ \theta_i^A\end{pmatrix}=\begin{pmatrix}\Delta x\\ \Delta y\\ \Delta\theta\end{pmatrix}+\begin{pmatrix}\cos\Delta\theta & \sin\Delta\theta & 0\\ \sin\Delta\theta & -\cos\Delta\theta & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}x_i-x^d\\ y_i-y^d\\ \theta_i-\theta^d\end{pmatrix} \tag{9-11}$$

其中，上标 A 表示对准后的特征，经过式(9-11)变换后，待配准的细节点特征便可与参考特征处于同一个参考系中。在本书中使用 Tico 描述子的概率密度值最大的细节点对作为初始对准点，并计算平移与旋转参数。经过配准后，接下来需要确定细节点间的对应关系，同时统计两幅指纹图像中可以匹配的细节点对的个数。在寻找匹配细节点对的时候可以加入贪婪算法和使用界限盒的方法来确保细节点对匹配成功率。

为了提高匹配准确度，将一副指纹图像作为参考图像进行一次匹配，再作为待配准图像进行一次匹配，分别计算能配对成功的细节点个数，最终匹配分数 MS 的计算公式如下：

$$\mathrm{MS}=\frac{1}{A_B B_A}\left[\sum_{(i,j)\in C}S(a_i,b_j)\right]^2 \tag{9-12}$$

这里需要注意的是，在对准时可以在很多对相似度都较高的细节点中多次选择初始配准点，计算它们各自的匹配分数，并选择最优的匹配结果，这样能够更进一步提高算法的性能。

Tico 描述子最终的匹配效果如图 9-14 所示，可以看到绝大部分的对应细节点都得到了正确的匹配。

值得一提的是，在处理形变较大或者来自不同采集仪的指纹图像时，与常规的只是用细节点的位置和方向进行匹配相比，使用 Tico 描述进行匹配所得到的结果更好，图 9-15 给出了不使用 Tico 描述子和使用 Tico 描述子对不同采集仪获得的指纹的匹配结果，可以看出，使用 Tico 描述子之后，匹配的结果得到了提升。

可以看出，在使用了细节点信息的同时使用方向场信息，能够更为准确的找到匹配的

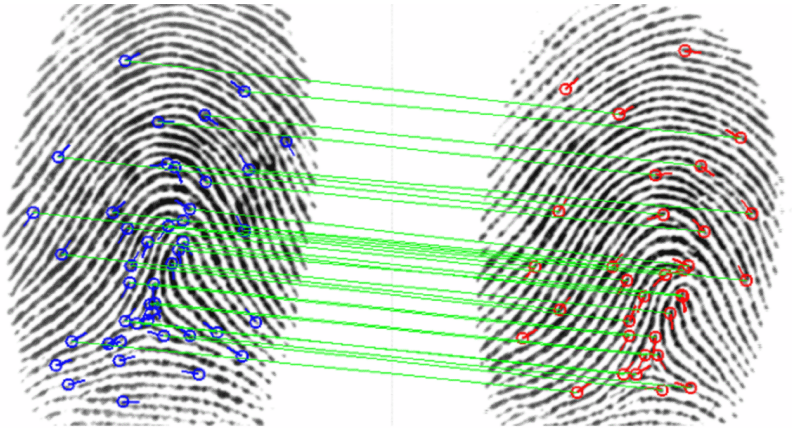
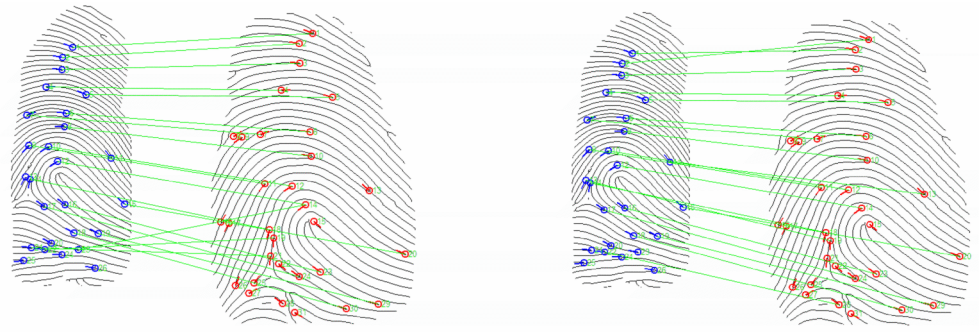


图 9-14　使用 Tico 描述子匹配的常规指纹图像



(a) 没有使用 Tico 算子　　(b) 使用了 Tico 算子

图 9-15　来自不同采集仪的指纹图像的匹配结果

细节点,同时对指纹图像的旋转和平移有更好的鲁棒性。

9.4　本章小结

本章介绍了指纹图像特征提取与匹配的方法,并对特征提取中应用链码(Chain-Code)进行指纹特征提取和应用方向场描述子(Tico)进行指纹特征匹配的方法做了详细的介绍。这两种方法分别在特征提取和匹配中都有着不错的性能表现,可以在实时的自动指纹识别系统中应用。

随着指纹识别在日常生活中的广泛应用,人们对指纹识别精度和识别速度的要求也越来越高,为了满足人们的需求,性能更高的指纹特征提取算法与匹配算法也正在研究中。

习题与思考题

1. 指纹图像的全局特征和局部特征有哪些？这两种特征在指纹识别中的作用分别是什么？
2. 常用的指纹特征提取的方法有哪些？它们分别有什么优缺点？
3. 在细化图中提取指纹细节点时，如何区分终结点和分叉点？
4. 指纹图像中的奇异点有什么特点？试着给出一种奇异点提取算法。
5. Tico 描述子的特点是什么？为什么 Tico 描述子更适合于来自不同采集仪所采集指纹图像的识别？

第 10 章　生物特征加密技术

在对生物特征识别技术有了全面的了解之后，本章将详细介绍生物特征加密技术的发展过程、以及与密钥保护相关的常用生物特征加密方法。并且，以模糊保险箱算法为例，详细的介绍生物特征加密的完整过程，最后给出了一个指纹识别加密的实例。

本章内容：10.1 节介绍了生物特征加密技术发展概述，10.2 节介绍常规指纹识别算法的评价方法，10.3 节介绍应用级指纹识别算法的评价方法，10.4 节总结本章的内容。

10.1　生物特征加密技术发展概述

生物特征其本身的唯一性和不变性是一把双刃剑，一方面，它可以保证我们的身份唯一，但另一方面，由于目前的识别技术需要存储生物特征模板，模板一旦泄露或丢失，就无法像银行卡那样更改或挂失。以指纹为例，传统的指纹识别系统大部分采用细节点作为识别特征，并且把细节点位置存储到模板中用于匹配。但系统若不采用任何加密措施确保数据库安全，整个指纹识别系统的安全性就无法得到保障，从而使得用户身份的安全性和隐私性受到威胁。从图 10-1 中可以看出，攻击模板就可以通过指纹识别系统的验证，从而危及到系统的安全性。指纹识别系统中的其它部分也可能遭受攻击，本章主要介绍指纹模板部分的保护。

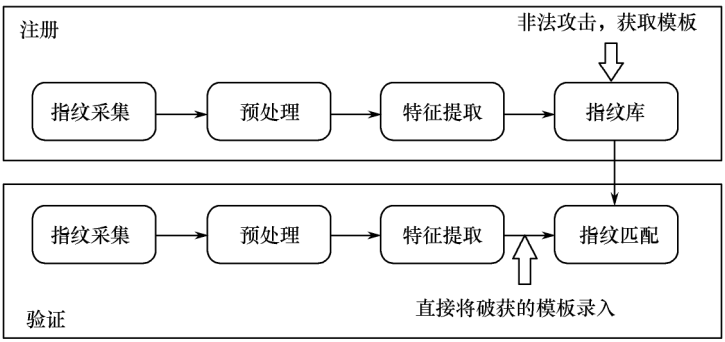


图 10-1　自动指纹系统可能受到攻击的部分

由于安全性问题，当下有关于指纹识别的应用几乎都是离线独立使用的，如指纹识别签到机、计算机指纹开机系统，以及手机上应用的指纹解锁功能等，但随着物联网、云计算与大数据电子商务等领域的发展需求，将生物特征识别技术安全的应用在这些领域的方案有很大的意义，因此，生物特征加密技术的研究和应用是迫切需要的。

1994 年，加拿大的 Dr. George Tomoko 首先结合指纹提出了生物特征加密(Biometric Encryption)这一概念，并申请了相关专利。在国内方面，王星名在 1999 年将加密概念引入了生物特征识别中，并进行了开创性研究。表 10-1 给出了生物特征加密技术发展历程和主要研究成果。

表 10-1　生物特征加密技术方案

主要作者	方案
George Tomoko	提出生物特征加密概念
Soutar	提出了一个生物特征加密的算法版本，主要是用傅里叶处理来补偿指纹图像的位移变换
Bjorn	提出了加入“幽灵点”来隐藏真实细节点
Davida	提出了“私有模板”的概念
Monrose	提出了“生物特征强化密码”的概念
Juels	提出了模糊承诺策略
Janbandhu	直接从生物特征模板形成生物特征签名，并使用了标准加密算法，如 RSA 和 DSA，密钥能够改变
Juels 和 Sudan	提出了“模糊保险箱”策略
Clancy	基于“模糊保险箱”提出了“指纹保险箱”策略
Uludag	提出了“指纹模糊保险箱”策略，提出了加密域配准和 Helper data 等概念
Hao	对虹膜识别应用模糊承诺策略，FAR 达到 0.47%

从表中可以看出生物特征加密技术的方案从理论研究逐渐发展到实际应用。在我国，中科院自动化研究所的田捷研究员对生物特征加密进行了深入的研究。在生物特征加密技术中，生物特征与密钥结合是最为常用的手段，下一节我们主要介绍与密钥有关的生物特征加密方法。

10.2　生物特征与密钥结合的常用方法

根据密钥使用的方式或产生的方式不同，生物特征识别领域中与密钥相关的思想和方法大致分为三类：密钥释放（Key Release）、密钥绑定（Key Binding）和密钥生成（Key Generation）。

1. 密钥释放（Key Release）

密钥释放的方法原理简单，用户选定好一个密钥，然后输入自己的生物特征，系统将密钥和生物特征简单的叠加在一起存储为一个混合模板，这个混合只是简单的拼接或合并，并没有其它复杂的操作，在需要输出密钥时，只需要将混合模板中的特征模板取出来与实时采集的特征进行比对，如果比对通过就将混合模板中的密钥提取出来，图 10-2 给出了密钥释放方法的步骤。

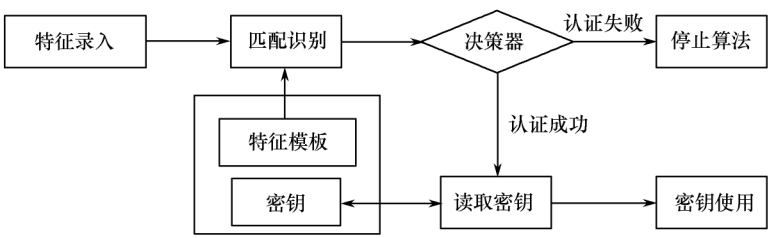


图 10-2　密钥释放方法的流程图

从图 10-2 中可以看出，密钥释放方法中密钥和生物特征模板只是简单地链接在了一起，密钥释放的方法很难抵御对模板的蓄意攻击，如果模板数据库被破获，用户的生物特征信息和密钥都将丢失。尽管如此，一些基于指纹的 USB-Key 产品已经生产并投入了市场，在电子政务、银行系统等一些领域得到了应用。口令与指纹识别 USB 设备结合，在某种意义上达到了双因子认证(指纹＋令牌)的效果，如果不同时泄露口令或 USB 设备，这种产品还是有较高的安全性。Moon 等人就在其发表的论文中详细地讨论了基于指纹的身份令牌的硬件要求和软件构架。

2. 密钥绑定(Key Binding)

密钥绑定的方法的原理与密钥释放的方法相似，不同点在于混合模板的生成方式不同。密钥绑定的方法是将用户的生物特征信息与密钥信息进行一些相对复杂的数学运算，或密码技术上的混合处理，生成模板保存起来，此模板不需要秘密保存，是在数据库模板中把生物特征数据和密钥数据以某种方式有机结合到一起，当生物特征匹配成功的时候密钥被以相应解绑算法提取出来，再加以使用，密钥绑定方法的流程如图 10-3 所示。Uludag 等人首先提出了在加密域内对指纹图像进行计算机自动配准，该方法的基本思想就是从指纹图像中提取 Helper Data 用以配准。Helper Data 的选取标准是既能反映指纹的部分本质特征但凭借这些特征又不足以恢复到原始的指纹图像或者用以识别的其它特征。

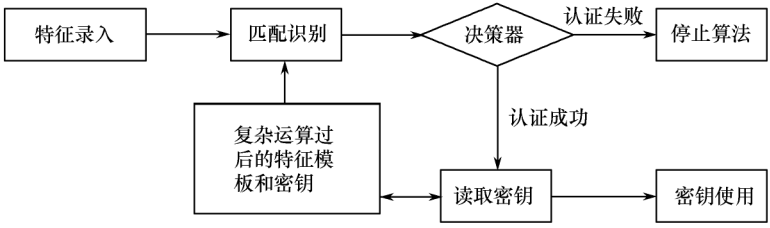


图 10-3　密钥绑定方法流程图

密钥绑定中，使用较为广泛的方法是 Juels 与 Sudan 在 2002 年提出的模糊保险箱(fuzzy vault)方法，模糊保险箱算法是生物特征加密领域的经典算法之一，很多其它的特征加密算法都是基于这个算法实现的。模糊保险箱算法整体分为加密、配准和解密三个模块。下一节将对 fuzzy vault 方法进行详细介绍。

3. 密钥生成(Key Generation)

上文中介绍的两种生物特征加密方法都是采用将特征和密钥结合的方式，所以需要用户事先提供密钥，然后和生物特征以某种方式结合在一起，生物特征认证成功，原有密钥就会被释放，从而可以进行后续的应用。如果生物特征和密钥结合的方式不是十分理想，导致密钥在认证过程中起主导作用的话，那么整个系统的安全性就是基于密钥的，一旦密钥丢失，系统的安全性则无法保障，甚至还可能会泄露生物特征信息。

密钥生成的方法避免了前期人为提供密钥的不足，密钥是由输入的生物特征数据直接生成的，或者是添加少量的辅助数据融合后生成的，即密钥数据主要来自于输入的生物特征信息，输入不同的生物特征信息产生的密钥不同。生成密钥的方式不是随意的，根据密码学对密钥的基本要求，生物特征生成的密钥需要满足以下几个要求。

模糊性：来自于同一个生物特征（如同一个手指）在限定的差异范围内生成的密钥相同，以保证每次验证同一个特征时密钥相同。

个体差异性：来自于不同的生物特征不可以生成相同的密钥。

安全性：生物特征生成的密钥需要满足密钥长度的要求，并且，当生物特征或密钥中其中一种不慎泄漏时，不能造成另外一种数据的同时泄露。

对密钥生成方法的研究还不算成熟，但这种方法由于密钥是生成的相对于其它两种方法更为便捷，也更加安全，将会是未来生物特征加密的一个热点方向。

10.3　模糊保险箱算法介绍

模糊保险箱（Fuzzy Vault）算法是生物特征加密领域最为经典的实用化算法，它是密钥绑定方法中的一种。这个算法是由 A. Juels 和 M. Sudan 在 2002 年提出来的，很多研究生物特征加密的研究者都是以这个算法为基础进行深入研究的。模糊保险箱算法的特点在于它把生物特征的模糊性和密码算法的精确性很好地结合起来。简单来讲，算法的原理可以分为以下两步。

加密阶段：用户 Alice 将秘密 K 放到保险箱（Vault）中，并用无序集 A 加以锁定。

解密阶段：用户 Bob 使用无序集 B 尝试打开保险箱访问 K。Bob 能够访问到 K 的充分必要条件是 Bob 的无序集 B 与 Alice 的无序集 A 的绝大多数元素重合。

模糊保险箱算法的具体实现过程如下。

生成保险箱：用户 Alice 选择关于 x 的多项式 p 来加密秘密 K，然后计算无序集 A 在多项式 p 上的投影 $p(A)$，这样 $(A, p(A))$ 就构成一个有限点集。然后随机生成一些杂凑点（Chaff Points）与之前生成的有限点集构成 Vault，也就是保险箱。这里需要注意的是，杂凑点的添加对于隐藏 K 非常必要，如果杂凑点添加得过少，那么攻击者很可能通过遍历的方式来暴力破解出秘密 K，所以在实际应用中杂凑点的数量需要比真实点多得多。

打开保险箱：用户 Bob 使用自己的无序集 B 去尝试打开保险箱 Vault，如果 B 和 A 绝大多数的元素重合，那么无序集 B 中有许多点就会落在多项式 p 上，使用纠错码技术，Bob 就能重构出 p 来，进而获取 K。但是如果 B 和 A 有相当大比例的元素不重合，那么 Bob 是基本上不可能重构出 p 的。

这个算法的安全性是基于多项式重构问题的。之所以特别适用于生物特征数据，是因为它使用无序集（如指纹的细节点信息就是无序集）工作，并且能够处理集合之间（元素数量和元素本身）的误差。

在模糊保险箱算法之后，很多研究者继续进行了研究，并结合了指纹等生物特征。Clancy 等人在 Juels 工作的基础上提出了指纹保险箱的概念，即注册阶段使用用户的指纹，并提取指纹的细节点的坐标作为输入。

Uludag 等人基于模糊保险箱和指纹保险箱提出了更为实用化的指纹模糊保险箱算法，其基本思想与上述两个研究者大致相同，但在细节上有所创新。下面介绍指纹模糊保险箱算法的流程。

首先使用循环冗余校检（CRC）对密钥 S 进行处理，就是 S 尾部加上特定位数的校验

码形成SC，然后使用SC按照一定的规则构造多项式函数p。与此同时，提取用于加密指纹模板图像的细节点位置信息(x,y)，级联横坐标和纵坐标$x||y$，并找到$x||y$在p上的投影点，随机添加一组不在P上并且距离真实细节点一定距离的杂凑点到保险箱中，就形成了最终的保险箱V，图10-4展示了指纹模糊保险箱的生成过程。

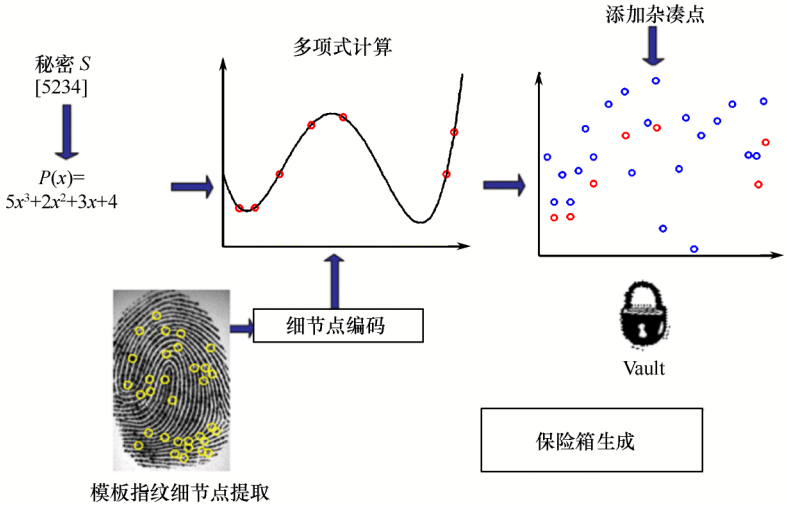


图10-4　指纹模糊保险箱的生成过程

访问保险箱时，首先提取实时采集的用于访问保险箱的指纹图像中细节点坐标信息(x,y)，级联横坐标和纵坐标$x \| y$，然后寻找保险箱V中与之对应的点，过滤掉杂凑点，找到一个可能是真实的点集，遍历这个点集中的所有点的多项式组合，使用拉格朗日插值法重构出相应的多项式，得到多组多项式系数集合，再用循环冗余校验(CRC)来确定哪一组是初始阶段加密的S，图10-5给出了指纹模糊保险箱的访问过程。

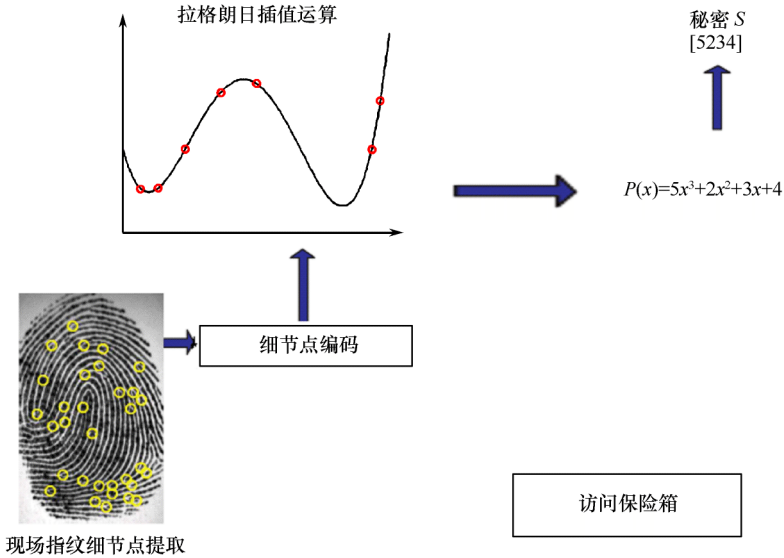


图10-5　指纹模糊保险箱的访问过程

上述与模糊保险箱有关的算法都是直接使用了人工专家配准后的细节点集进行测试，Uludag 等人率先提出了可以使用计算机自动配准指纹细节点方法，称之为加密域的匹配。该方法的原理是从模板指纹和实时指纹中各提取出 Helper data，Helper data 中存储了可以用来对两组细节点进行配准的信息，如指纹图像中的方向场流曲线信息，方向场流曲线反映了指纹脊线的走向，可以用作配准。在比对两幅指纹图像的 Helper data 之后得出旋转平移参数并配准，得到可能匹配的细节点集，再进行模糊保险箱的访问步骤。

加密域自动匹配的算法研究对实现完整的生物特征加密系统起着关键作用，目前该方向还需要进行深入的研究。本节介绍了模糊保险箱和相关算法的流程，下面我们具体介绍指纹模糊保险箱算法的设计与实现。

10.4　指纹模糊保险箱算法实现

本节介绍的一种基于指纹细节点的模糊保险箱算法使用了指纹的细节点信息与密钥进行绑定，算法包括加密和解密两个阶段，下面将详细的介绍每个阶段的算法实现。

10.4.1　加密阶段

加密阶段的主要步骤有指纹图像预处理、杂凑点添加、混合点集编码、构造多项式、生成保险箱等步骤。这里我们选择一个长度为 128 比特的任意密钥 S 作为待绑定密钥，其每一步的实现方法如下。

1. 指纹图像预处理

在指纹模糊保险箱算法中，对指纹图像进行预处理的目的是获得用于绑定密钥 S 的细节点特征集 $M=\{(x_i,y_i,\theta_i)\mid i=1,2,\cdots,N\}$，其中 N 是细节点的数目。预处理过程中涉及的图像增强、二值化以及特征提取等步骤可以参照本书第 7～9 章的相关内容。

2. 杂凑点添加

模糊保险箱算法中的重要一步就是添加杂凑点来保护真实细节点，这里我们随机生成一个杂凑点集 $C=\{(a_i,b_i,\omega_i)\mid i=1,2,\cdots,D\}$，其中 D 是杂凑点的数目。通常杂凑点的数目要远远大于真实细节点 N，这里我们取 $D\approx 10N$。杂凑点的添加除了要随机外还需要满足一定的条件：添加的杂凑点不可离真实细节点太近，通常给定一个距离阈值，随机生成的杂凑点需要通过该阈值判断；当有杂凑点的距离与阈值非常接近时，其随机生成的角度信息也一定要与真实细节点保持很大差异。得到上述杂凑点集 C 后，我们将 C 添加到真实细节点集 M 中，构成混合点集 H，H 中点的数量为 $D+N$。

3. 混合点集编码

在得到了由杂凑点和真实细节点共同构成的混合点集 H 后，将 H 中的每一个点的坐标信息级联，转换为 16 比特的字符串集 X，后续我们将使用编码后的混合点集来进行多项式的计算。

4. 构造多项式

构造多项式需要对密钥 S 首先进行处理，将 S 分为 8 个 16 比特的字符串，分别是 $r_1, r_2, \cdots, r_8$ 使用 16 位循环冗余校验 CRC-16 对 S 进行处理，得到 16 比特的字符串 r_0。$r_0, r_2, \cdots, r_8$ 就是多项式 P 的系数。P 最终表示为：

$$p(x)=r_8x^8+r_7x^7+\cdots+r_0 \tag{10-1}$$

得到多项式之后，就可以计算模糊保险箱了。

5. 生成保险箱

上边的步骤我们得到了编码后的混合点集和多项式，将字符串集 X 集中真实细节点的编码值带入 P 中计算得到 $p(x)$，将字符串集 X 中的伪细节点随机取 $P(x)$ 值，将两部分 $P(x)$，最终得到模糊保险 $V=\{(X_i, \quad p(X_i)) \mid i=1,2,\cdots,N+D\}$。

10.4.2 解密阶段

解密阶段的主要步骤有指纹图像预处理、杂凑点过滤、获得解密点集、重构多项式和解密密钥。下面分别介绍每一步的实现方法。

1. 指纹图像预处理

解密阶段需要实时采集用户指纹，从而获得实时指纹的细节点信息。图像预处理的方法同样是进行图像增强、二值化以及特征提取等步骤，具体方法可以参照本书第 7～9 章的相关内容。经过预处理后，我们得到新的细节点集 $M'=\{(x_i', y_i') \mid i=1,2,\cdots,N'\}$。

2. 杂凑点过滤

将 M' 与加密阶段生成的保险箱 V 进行比对，若实时采集的指纹与加密阶段的指纹来自于同一手指，那么理论上 M' 中会有一定数量的点与 V 中的点相近，从而加密时掺杂的杂凑点大部分会被过滤掉将筛选后 M' 中的点按照加密阶段的编码方工编码为 16 比特的字符串集 X'。

在杂凑点过滤阶段，需要根据加密时的细节点个数以及构建的多项式阶数来设定一个阈值，进行过滤后保留下来的点的个数若小于此阈值，则无法重构多项式，因此直接判定为解密失败；若过滤后的保留下来的点的个数大于此阈值，则这些点构成解密点集 T，T 将用于多项式的重构。

3. 重构多项式

由于加密和解密时两个指纹图像不是完全一样的，因此上一步我们得到解密点集 T，T 中元素为 (g, h)，T 不会完全由真实细节点构成，可能存在一些杂凑点。此时，我们从 T 中任选 9 个点带入拉格朗日插值公式中反求多项式系数，拉格朗日插值公式如下：

$$p'(x)=\frac{(x-g_2)(x-g_3)\cdots(x-g_9)}{(g_1-g_2)(g_1-g_3)\cdots(g_1-g_9)}h_1+$$
$$\frac{(x-g_1)(x-g_3)\cdots(x-g_9)}{(g_2-g_1)(g_2-g_3)\cdots(g_2-g_9)}h_2+\cdots+$$

$$\frac{(x-g_1)(x-g_2)\cdots(x-g_8)}{(g_9-g_1)(g_9-g_2)\cdots(g_9-g_8)}h_9 \tag{10-2}$$

经过对式(10-2)求解后，每一组的 9 个点都可能得到一组多项式系数，但只有 9 个点都是真实细节点时获得的才是正确的多项式。对此，每求得一组多项式系数后，我们计算前 8 个系数的 CRC 校验码，看是否与第 9 个系数相等，若相等，才是正确的多项式系数。至此我们重构出的多项式 $p'(x)$ 如下：

$$p'(x)=r'_8x^8+r'_7x^7+r'_6x^6+\cdots+r'_1x+r'_0 \tag{10-3}$$

得到多项式后，我们就可以根据系数获得密钥 S 了。

4. 解密密钥

根据上一步得到的多项式系数 $r'_0,r'_1,\cdots,r'_8$，用加密阶段中处理密钥的方法重新获得密钥 S，至此我们解密出了密钥 S。

本节我们完整的介绍了指纹模糊保险箱算法的计算过程，从构造过程中可以看出，仅凭借保险箱是无法获取密钥 S 和细节点 M 中的任何一种信息的，因此模糊保险箱算法是一种安全可靠的生物特征加密算法。

10.5　本章小结

本章主要介绍了生物特征加密技术的实现，首先分析了生物特征识别技术的不安全因素，然后介绍了密钥结合生物特征混合模板的几种保护方法，最后重点介绍了模糊保险箱算法和它所衍生的几种重要生物特征加密算法。

习题与思考题

1. 除了模板之外，生物特征识别系统还有哪些步骤是不安全的，易受攻击的？
2. 请思考除多项式计算之外是否还有其它复杂运算能够满足密钥绑定方法的安全需求算法安全强度如何评估？
3. 模糊保险箱算法生成的保险箱能否被暴力破解出多项式系数从而还原出密钥呢？
4. 在指纹模糊保险箱算法中，除了细节点信息，你还能想到哪些信息可以用于保险箱的生成？
5. 请思考加密域配准的难点所在。

第 11 章　生物特征识别与加密技术的典型应用

生物特征识别技术由于其具有唯一性等特点，最早被应用于司法公安系统，主要作为刑侦破案的证物，但随着计算机技术的发展，生物特征识别技术已经成熟地应用在各个领域。为保证生物特征识别技术在各领域中的安全应用，生物特征加密技术也渐渐地成为研究和应用的热点。本章将介绍生物特征识别与加密技术在电子政务、电子商务、移动终端认证等领域的最新应用，并展望未来的发展趋势。

本章内容：11.1 节介绍生物特征识别与加密技术在电子政务领域的应用，11.2 节介绍生物特征识别与加密技术在移动终端中的应用，11.3 节介绍生物特征识别与加密技术在电子商务领域的应用，11.4 节为生物特征加密技术的未来应用展望，11.5 节总结本章的内容。

11.1　电子政务领域的应用

生物特征识别技术在电子政务领域中的应用已经十分广泛，例如，公民身份的管理控制，国家出入境人员的管理等。最为典型的政府应用案例——美国的访客计划（US-VISIT），该计划部署于美国所有出入境口岸，年处理人次量超 4 亿，已经成为美国反恐的重要组成部分。图 11-1 是访客计划的宣传图片和采集现场。

图 11-1　美国访客计划

在我国，公民使用的第二代身份证中含有科技含量较高的芯片，其中不仅存放了公民的个人信息，而且预留了存放指纹、血型等生物特征的空间。很多地区已经开始采集公民的指纹信息并与身份证融合。图 11-2 是我国民警在采集公民的指纹信息并录入身份证中。

生物特征识别技术应用在电子政务领域会极大地提高政务的办公效率，并在出入境、户籍管理等方面为公民带来更为方便快捷的个人身份认证方法。

图 11-2　我国公民在采集指纹

11.2　移动终端的应用

生物特征识别技术不仅在电子政务领域为人们带来了便捷，在移动终端应用中的个人身份认证方面也表现出色，尤其是手机端的指纹认证系统，已经被各大手机厂商和芯片厂商应用在其主打的旗舰手机中。

人机接口 IC(智能卡)在智能手机市场的应用如火如荼，指纹识别作为现阶段旗舰手机的标配成为手机制造商手中的大卖点，为移动支付提供了后续服务。业内预估 2014 年搭载指纹辨识的人机接口 IC 将较 2013 年成长 5 倍，并在未来两年内约有八成的年复合成长率。指纹识别芯片成为各家 IC 设计厂商兵家必争之地。这其中，既包括了海外的 AuthenTec(隶属于苹果公司)、新思 Synaptics、指纹卡(Fingerprint Cards，FPC)，台湾地区的 F－敦泰、义隆，其它厂商还有茂丞科技、盛群等。此外，中国内地的 Goodix 汇顶科技在近几年也得到了很好的发展。

汇顶科技成立于 2002 年，于 2006 年开始进军触控行业，具有丰富的电容触摸芯片的量产经验，已拥有电容触控技术专利超过 30 项，目前是联发科唯一战略合作伙伴，其市场上量产应用的手机是魅族 MX4 Pro，MX4 Pro 是国内手机厂商正面按压式指纹识别方案的首创。如图 11-3 所示，全世界各大主流手机厂商的旗舰机均配置了指纹识别模块，包括苹果的 iPhone 5s/6/6Plus、三星的 Galaxy5/6、华为的 Mate7，等等。

图 11-3　搭载了指纹识别模块的 iPhone6 及华为 Mate7

我们不难预测,生物特征识别技术将是未来智能手机上不可或缺的一个重要组成模块,将会为移动个人认证带来极大的方便。

11.3 电子商务的应用

指纹识别系统在移动终端上的成功应用也给用户带来了全新的移动支付方式,其中的佼佼者当属苹果公司的 Apple Pay。截至 2014 年 3 月 7 日,苹果公司宣布 Apple Pay 已与世界范围内的 2500 家银行合作,70 多万个零售机构接受 Apple Pay。另外,阿里巴巴公司开发的阿里云 OS 手机也搭配了指纹识别模块,可以直通支付软件支付宝进行付款。图 11-4 是阿里云 OS 手机中搭载了指纹识别模块的支付界面。

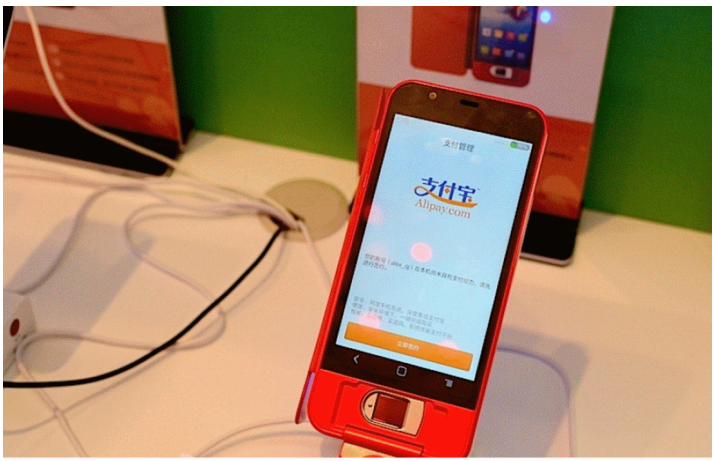


图 11-4 搭载指纹识别模块的阿里云 OS 手机

目前,支付宝、部分银行的手机银行已经都可以支持手机自带的指纹识别支付功能,其应用领域将越来越广,未来带给人们的便利也越来越多。

11.4 应用展望

由上述章节可知,生物特征识别与加密技术已经成熟的应用在日常生活中的各个领域,而随着生物特征识别与加密技术的发展,其应用前景也将越来越广阔,下边给出一些生物特征识别与加密技术的潜在应用:

公安机关户籍管理中的应用。我国是世界上人口最大的国家,户籍管理是一个很大的问题,人口众多,流动人口大,户籍管理难免出现漏洞。我们经常从新闻中听说某人拥有多个身份和户籍信息。如果将生物特征识别技术应用于公安机关的户籍管理网络,如从入籍开始,就采集该公民的十指指纹信息,那么该信息一旦记录在档案中,就不可以再次进行户籍的注册,在办理户籍更改等业务时,同样需要指纹通过,这样就杜绝了多重户籍、有户无人或有人无户的情况。

人口普查的应用。如果普及了生物特征识别技术,那么人口普查时即便重复的录入

的某人的信息,但通过指纹比对,也可过滤掉重复的信息,为人口普查带来便捷。除此之外,生物特征识别技术在刑侦破案、出入境管理等等很多领域还有很大的应用前景。

上述的多种应用都对生物特征数据库安全有着严格的要求,因此生物特征加密技术还需要进行不断地研究和探索,以满足更多的应用需求。

11.5　本章小结

本章主要介绍了生物特征识别加密技术在电子政务、移动终端和电子商务领域的最新应用。不难预见,未来生物特征加密的市场前景将更为广阔,给用户带来的使用体验也将越来越好。

习题与思考题

1. 你认为私营公司可以被允许采集用户的指纹吗,为什么?
2. 在众多的生物特征识别技术中,哪一种是你最希望在手机上见到的?
3. 你会放心的使用生物特征作为认证方式来进行支付吗? 为什么?
4. 思考未来生物特征加密技术可能出现的其它应用。
5. 思考生物特征的应用会为公安机关的户籍管理和身份证系统带来什么好处。还面临哪些困难?
6. 近来通信行业的三大运营商均要求用户使用实名制开户,你认为生物特征能否应用在实名制过程中,或者完全代替 SIM 卡,为什么?
7. 如果银行可以使用生物特征来办理存取款或其它业务,你觉得在这个过程中需要注意什么,为什么?

附录 A　专有名词缩略语

AES（Advanced Encryption Standard）　高级加密标准
AFIS（Automatic Fingerprint Identification System）　自动指纹识别系统
AGNES（Agglomerative NESting）　层次聚类方法
ANSI（American National Standards Institute）　美国国家标准协会
BAC2005（Biometrics Authentication Competition 2005）
　　2005 年中国科学院自动化所联合组织举办的生物特征识别竞赛
BVC（Biometrics Verification Competition）　中国科学院自动化所联合组织举办的生物特征识别竞赛
Biometric Encryption　生物特征加密
CCD（Charged Coupled Device）　电荷耦合元件
Chaff Points　杂凑点
ChainCode　链码
CMOSE（Complementary Metal Oxide Semiconductor）　互补金属氧化物半导体
Core　中心点
Coherence　方向一致性
CRC（Cyclic Redundancy Check）　循环冗余校检
CRT（Cathode Ray Tube）　阴极射线管
DFT（Discrete Fourier Transform）　离散傅里叶变换
DPI（Dots Per Inch）　分辨率
EER（Equal-Error Rate）　等错误率
FAR（False Acceptance Rate）　误识率
FBI（Federal Bureau of Investigation）　美国联邦调查局
FFT（Fast Fourier Transformation）　快速傅里叶变换
FIR（Finite Impulse Response）　直接型有限长单位冲激响应
Fourier transform　傅里叶变换
FRR（False Rejection Rate）　拒识率
FTA（Failure to Capture）　捕获失败
FTD（Failure to Detect）　指纹获取模块中的探测失败
FTE（Failure to Enroll）　模板创建过程中的注册失败
FTP（Failure to Process）　特征提取模块中的处理失败
Fuzzy Vault　模糊保险箱
FVC（Fingerprint Verification Competition）　指纹识别大赛
Hough transform　霍夫变换
IAFIS（The Integrated Automated Fingerprint Identification System）
　　犯罪记录查找系统
IAPR（International Association of Pattern Recognition）　国际模式识别协会
Key Release　密钥释放

Key Binding　密钥绑定
Key Generation 密钥生成
LED (Light Emitting Diode)　发光二极管
Level 1　一级特征
Level 2　二级特征
Level 3　三级特征
LMS (Least mean square)　最小均方算法
Mean　灰度均值
Mean filter　均值滤波
MMSE (Minimum Mean Square Error)　最小均方误差
MOS (Mean Opinion Score)　主观质量评分法
MSE (Mean Square Error)　均方误差
NIST (National Institute of Standards and Technology)
　　美国国家标准与技术研究院
Orientation Image　指纹方向图
Petabytes　皮比特
Ridge　脊线
Ridge Frequency　脊线频率
Ridge Orientation　脊线方向
ROC 曲线 (Receiver Operator characteristic Curve)　受试者工作特征曲线
Single-1ink　单链接
Singular Regions　奇异区域
STFT (Short-time Fourier transform)　短时傅里叶变换
Unique Identification Project (也称"Aadhar"计划)　印度的身份识别项目
US-VISIT (the United States Visitor and Immigrant Status Indicator Technology)
　　美国访客暨移民身份显示系统
XDFinger 数据库　西安电子科技大学指纹数据库
Valley　谷线
Variance　方差

附录B　符 号 表

∂	求导数
θ_{xy}	点(x,y)处的脊线方向
$\int$	求积法
$\sum$	求和
$*$	卷积
$[\ ]^T$	矩阵的转置
$\arccos\theta$	反余弦函数
$a \cdot b$	a，b 向量点乘
$A \otimes B$	B 对 A 进行腐蚀
$A \oplus B$	B 对 A 进行膨胀
$\cos\theta$	余弦函数
$E(a)$	求 a 的期望
f_{xy}	点(x,y)的脊线频率
$I(x,y)$	点(x,y)处的灰度值
log	求对数
$\min(a,b)$	求 a，b 中的最小值
$\sin\theta$	正弦函数
$\tan^{-1}\theta$	正弦函数的反函数
x—signature	x 的坐标值
(x,y)	图像中的坐标位置

参 考 文 献

[1] Afsar F, Arif M, Hussain M. An effective approach to fingerprint segmentation using fisher basis. The 9th International Multitopic Conference, Karachi, 2005:1-6

[2] Akram M U, Nasir S, Tariq A, et al. Improved fingerprint image segmentation using new modified gradient based technique. Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on. IEEE, 2008: 001967-001972

[3] Baig A, Bouridane A, and Kurugollu F. A corner strength based Fingerprint segmentation algorithm with dynamic thresholding. The 19th International Conference on Pattern Recognition, Tampa, 2008:1-4

[4] Banner C, Stock R. FBI'S (FEDERAL BUREAU OF INVESTIGATION'S) APPROACH TO AUTOMATIC FINGERPRINT IDENTIFICATION, PART 2. FBI Law Enforcement Bulletin, 1975, 44(2): 26-31

[5] Barequet G, Har-Peled S. Efficiently approximating the minimum-volume bounding box of a point set in three dimensions. Journal of Algorithms. 2001,38(1):91-109

[6] Bazen A M, Gerez S H. Segmentation of fingerprint images. Proc. Workshop on Circuits Systems and Signal Processing (ProRISC 2001). 2001, 276-280

[7] Bovik A C. Handbook of image and video processing. Academic press, 2010

Bringer J, Chabanne H, Cohen G, et al. Theoretical and practical boundaries of binary secure sketches. Information Forensics and Security, IEEE Transactions on, 2008, 3(4): 673-683

[8] Candela G, Grother P, Watson C, Wilkinson R, Wilson C. PCASYS-a pattern-level classification automation system for fingerprints. NIST technical report NISTIR. 1995,5647

[9] Cappelli R, Maio D, Maltoni D. Modelling plastic distortion in fingerprint images. Advances in Pattern Recognition—ICAPR 2001: Springer; 2001. p. 371-8

[10] Cavoukian A, Stoianov A. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy. Information and Privacy Commissioner, Ontario, 2007

[11] Champod C, Lennard C J, Margot P, et al. Fingerprints and other ridge skin impressions. CRC press, 2004

[12] Chen X J, Tian J, Cheng J G, et al. Segmentation of finger-print images using linear classifer.

EURASIP Journal on Applied Signal Processing, 2004(4):480-494

[13] Chen Y, Dass S C, Jain A K. Fingerprint quality indices for predicting authentication performance audio-and video-based biometric person authentication. Springer Berlin Heidelberg, 2005: 160-170.

[14] Chikkerur S, Carteright A N, Govindaraju V. Fingerprint enhancement using STFT analysis. Pattern Recognition, 40 (2007) 198-211

[15] Datta A, Parui S K. A robust parallel thinning algorithm for binary images. Pattern recognition. 1994,27(9):1181-92

[16] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Advances in cryptology-Eurocrypt 2004. Springer Berlin Heidelberg, 2004: 523-540

[17] Draper S C, Khisti A, Martinian E, et al. Using distributed source coding to secure fingerprint biometrics. Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on. IEEE, 2007, 2: II-129-II-132

[18] Frassen T, Zhou X, Busch C. Fuzzy Vault for 3D face recognition systems. Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on. IEEE, 2008: 1069-1074

[19] Golic′ J D, Baltatu M. Entropy analysis and new constructions of biometric key generation systems. Information Theory, IEEE Transactions on, 2008, 54(5): 2026-2040

[20] Gottschlich C. Curved-region-based ridge frequency estimation and curved gabor filters for fingerprint image enhancement. IEEE Transactions on Image Processing, 2012, 21(4):2220-2227

[21] Greenberg S, Aladjem M, Kogan D, et al. Fingerprint image enhancement using filtering techniques. Pattern Recognition, 2000. Proceedings. 15th International Conference on. IEEE, 2000, 3: 322-325

[22] Hao F, Anderson R, Daugman J. Combining crypto with biometrics effectively. Computers, IEEE Transactions on, 2006, 55(9): 1081-1088

[23] Hong L, Jain A K. Fingerprint enhancement. Automatic Fingerprint Recognition Systems: Springer; 2004. p. 127-43

[24] Hong L, Wan Y, Jain A K. Fingerprint image enhancement: algorithm and performance evaluation. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 1998, 20(8): 777-789

[25] Hong L. Automatic personal identification using fingerprints: Michigan State University; 1998

[26] Jain A K, Hong L, Bolle R. On-line fingerprint verification. Pattern Analysis and Machine Intelligence, IEEE Transactions on. 1997,19(4):302-14

[27] Jain A K, Hong L, Pankanti S, Bolle R. An identity-authentication system using fingerprints. Proceedings of the IEEE. 1997,85(9):1365-88

[28] Jain A K, Nandakumar K, Nagar A. Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008, 2008: 113

[29] Jain A K, Ross A, Prabhakar S. Fingerprint matching using minutiae and texture features. Image Processing, 2001 Proceedings 2001 International Conference on, F, 2001. IEEE

[30] Jang J, Elliott S J, Kim H. On improving interoperability of fingerprint recognition using resolution compensation based on sensor evaluation. Advances in Biometrics: Springer; 2007. p. 455-63

[31] Jiang X, Yau W Y, Ser W. Detecting the fingerprint minutiae by adaptive tracing the gray-level ridge. Pattern Recognition, 2001, 34(5): 999-1013

[32] Jiang X, Yau W Y. Fingerprint minutiae matching based on the local and global structures. Pattern Recognition, 2000 Proceedings 15th International Conference on; 2000: IEEE

[33] Jiang X. Fingerprint image ridge frequency estimation by higher order spectrum. Image Processing, 2000 Proceedings 2000 International Conference on; 2000: IEEE

[34] Juels A, Sudan M. A fuzzy vault scheme. Designs, Codes and Cryptography, 2006, 38(2): 237-257

[35] Juels A, Wattenberg M. A fuzzy commitment scheme. Proceedings of the 6th ACM conference on Computer and communications security. ACM, 1999: 28-36

[36] Klein S, Bazen A M, Veldhuis R. Fingerprint image segmentation based on hidden Markov models. The 13th Annual Workshop on Circuits, Systems, and Signal Processing, Veldhoven, 2002:310-318

[37] Lee H C, Ramotowski R, Gaensslen R. Advances in fingerprint technology: CRC press; 2001

[38] Lee Y J, Bae K, Lee S J, et al. Biometric key binding: Fuzzy vault based on iris images. Advances in Biometrics. Springer Berlin Heidelberg, 2007: 800-808

[39] Lee Y J, Park K R, Lee S J, et al. A new method for generating an invariant iris private key based on the fuzzy vault system. Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 2008, 38(5): 1302-1313

[40] Liu E Y, Zhao H, Guo F F, et al. Fingerprint segmentation based on an adaBoost classifier. Frontiers of Computer Science in China, 2011,5(2): 148-157

[41] Maio D, Maltoni D. Direct gray-scale minutiae detection in fingerprints. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 1997, 19(1): 27-40

[42] Maltoni D, Maio D, Jain A K, et al. Handbook of fingerprint recognition. Springer Science & Business Media, 2009

[43] Mao K M, Zhu Z L, Deng Z F. Fingerprint Core Point Detection based on SVM and Complex Filter. Advances in information sciences and service sciences, 2011, 3(8): 85-96

[44] Marques A C P B, Thome A C G. A neural network fingerprint segmentation method. Hybrid Intelligent Systems, 2005. HIS'05. 5th International Conference on. IEEE, 2005: 6 pp

[45] Nagar A, Nandakumar K, Jain A K. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recognition Letters, 2010, 31(8): 733-741

[46] Nandakumar K, Jain A K, Pankanti S. Fingerprint-based fuzzy vault: Implementation and performance. Information Forensics and Security, IEEE Transactions on, 2007, 2(4): 744-757

[47] Phillips P J, Martin A, Wilson C L, Przybocki M. An introduction evaluating biometric systems. Computer. 2000, 33(2): 56-63

[48] Raicevic A M, Popovic B M. An effective and robust fingerprint enhancement by adaptive filtering in frequency domain. Facta Universitatis(NIS) Ser: Elec Energ, 2009, 22(1): 91-104

[49] Ratha N K, Karu K, Chen S, et al. A real-time matching system for large fingerprint databases. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 1996, 18(8): 799-813

[50] Ross A, Jain A K. Information fusion in biometrics. Pattern recognition letters. 2003, 24(13): 2115-25

[51] Ross A, Nadgir R. A thin-plate spline calibration model for fingerprint sensor interoperability. Knowledge and Data Engineering, IEEE Transactions on. 2008, 20(8): 1097-110

[52] Simon-Zorita D, Ortega-Garcia J, Cruz-Llanas S, et al. An improved image enhancement scheme for fingerprint minutiae extraction in biometric identification. Audio-and Video-Based Biometric Person Authentication. Springer Berlin Heidelberg, 2001: 217-223

[53] Tian Q C, Wang Q l. An Adaptive Fingerprint image enhancement algorithm based on frequency domain filter. Interntinal Journal of Intelligent Information Processing, 2013. 4(1): 32-39

[54] Tico M, Kuosmanen P. Fingerprint matching using an orientation-based minutia descriptor. Pattern Analysis and Machine Intelligence, IEEE Transactions on. 2003, 25(8): 1009-14

[55] Tomko G J, Soutar C, Schmidt G J. Fingerprint ctrolled public key cryptographic system. U. S. Patent 5541994, July 30, 1996 (Priority date : Sept. 7, 1994)

[56] Tuyls P, Akkermans A H M, Kevenaar T A M, et al. Practical biometric authentication with template protection. Audio-and Video-Based Biometric Person Authentication. Springer Berlin Heidelberg, 2005: 436-446

[57] Vizcaya P R, Gerhardt L A. Multiresolution fuzzy approach for singularity detection in fingerprint images. Enabling Technologies for Law Enforcement and Security. International Society for Optics

and Photonics, 1997: 46-56

[58] Wahab A, Chin S H, Tan E C. Novel approach to automated fingerprint recognition. Image and Signal Processing, IEE Proceedings-. IET, 1998, 145(3): 160-166.

[59] Wang H, Yan S, Liu J, Tang X, Huang TS. Correspondence propagation with weak priors. Image Processing, IEEE Transactions on. 2009,18(1):140-50

[60] Wu C, Tulyakov S, Govindaraju V. Robust point-based feature fingerprint segmentation algorithm. Advances in Biometrics. Springer Berlin Heidelberg, 2007: 1095-1103

[61] X. Zhan, Z. Sun, Y. Yin. A Method Based on the Markov Chain Monte Carlo for Fingerprint Image Segmentation. Fuzzy Systems and Knowledge Discovery: Second International Conference, Changsha, 2005:240-248

[62] Yin J, Zhu E, Yang X, et al. Two steps for fingerprint segmentation. Image and vision computing, 2007, 25(9): 1391-1403

[62] Yin Y, Wang Y, Yang X. Fingerprint image segmentation based on quadric surface model. Audio- and Video-Based Biometric Person Authentication. Springer Berlin Heidelberg, 2005: 647-655

[64] Zhang W, Wang Y. Core-based structure matching algorithm of fingerprint verification. Pattern Recognition, 2002 Proceedings 16th International Conference on; 2002: IEEE

[65] Zhang Z, Schwartz S, Wagner L, Miller W. A greedy algorithm for aligning DNA sequences. Journal of Computational biology. 2000,7(1-2):203-14

[66] Zhu E, Yin J P, Hu C F, et al. A systematic method for fingerprint ridge orientation estimation and image segmentation. Pattern Recognition, 2006,39(8): 1452-1472

[67] 敖山,马骏等. 生物特征识别系统安全性分析与思考. 微计算机信息,2007(23):

[68] 陈晖, 殷建平, 祝恩, 胡春风, 李永. 一种基于细节点局部描述子的指纹图像匹配方法. 计算机工程与科学. 2010(1):87-91

[69] 冈萨雷斯. 数字图像处理(第二版). 北京:电子工业出版社,2007

[70] 郭文娟, 杨公平, 董晋利. 指纹图像分割方法综述. 山东大学学报. 2010: 95-103

[71] 贾永红. 数字图像处理(第二版). 武汉:武汉大学出版社,2010

[72] 李亮, 田捷, 张阳阳, 杨鑫, 吴哲. 基于多型号指纹采集设备的指纹交叉比对算法. 全国网络与信息安全技术研讨会论文集 (下册). 2007

[73] 梅园. 自动指纹识别系统中若干关键问题研究. 南京:南京理工大学博士论文, 2009

[74] 庞辽军,裴庆祺,李慧贤. 信息安全工程. 西安:西安电子科技大学出版社,2010

[75] 任春晓, 尹义龙. 基于标记盒的指纹分割. 山东大学学报. 2006: 54-57

[76] 田捷, 陈新建, 张阳阳, 杨鑫, 何余良, 李亮, et al. 指纹识别技术的新进展. 自然科学进展.

2006,16(4):400-8

[77] 田捷, 杨鑫. 生物特征识别技术理论与应用. 北京:电子工业出版社, 2005

[78] 余松煜,周源华,张瑞. 数字图像处理. 上海:上海交通大学出版社,2007

[79] 张海春, 回文博, 林立忠. 指纹识别技术研究进展. 石家庄学院学报. 2005,7(3):25-8

[80] 张素文. 基于 DSP 的指纹采集系统的研究. 武汉:武汉理工大学,2006

[81] 赵小川. MATLAB 图像处理—能力提高与应用案例. 北京: 北京航空航天大学出版社,2014

[82] 周广通, 尹义龙, 郭文鹃. 基于协同训练的指纹图像分割算法. 山东大学学报. 2009: 22-26

[83] 祝恩,殷建平,张国敏,胡春风. 自动指纹识别技术. 长沙:国防科技大学出版社,2006